(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/08/2004

To: Office of the General Counsel **Attn:** Investigative Law Unit
Room 7326

International Operations **Attn:** IOS/IOU-2

b6
b7C

b2
b7E

From: [redacted]
Contact: [redacted], x[redacted]

b2
b6
b7C

Approved By: [redacted]

Drafted By: [redacted] whz

b6
b7C

Case ID #: 66F-HQ-C1364260-9 (Pending)
66F-HQ-C1384970 (Pending)

7645

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: This communication responds to the lead set for ALL RECEIVING OFFICES in the referenced communication.

Reference: 66F-HQ-C1364260 Serial 5

Details: The one incident that comes to mind concerning [redacted] is the Patriot Act Provisions to seize money in a corresponding bank account of a Middle Eastern bank. There was one Letters Rogatory from the DOJ-OIA including cases in which banking records were sought. [redacted] is a country with banking secrecy laws, and it is difficult to get financial records. However, when a bank in [redacted] has money in a corresponding account in a U.S. bank, it is possible to freeze the account until the information sought is obtained by the United States. This matter met with some limited success.

b2
b7E

[redacted] considers this lead covered.

COVERED
OTHER/YES

7326

66F-HQ-C1364260-EC

To: Office of the General Counsel From: [redacted]
Re: 66F-HQ-C1364[redacted], 03/08/2004

b2
b7E

LEAD(s):

Set Lead 1: (Info)

ALL RECEIVING OFFICES

For information only.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/09/2004

To: General Counsel **Attn:** Investigative Law Unit
[redacted] Room 7326

International Operations **Attn:** SSA [redacted] IOU-II

b6
b7C
b2

b2
b7E

From: [redacted]
Contact: [redacted]

Approved By: [redacted]

b6
b7C

Drafted By: [redacted]:ac

Case ID #: ~~66F~~-HQ-C1364260-14 (Pending)
66F-HQ-C1384970-18 (Pending)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: To provide results and cover lead.

Reference: 66F-HQ-C1364260 Serial 5

Details: For information of recipients, to date, [redacted] has not had the opportunity to use any of the investigative tools created by the USA PATRIOT ACT.

Consequently, [redacted] is negative for any feedback which is responsive to lead 66F-HQ-C1364260 Serial 5, and therefore considers above referenced lead covered.

b2
b7E

To: General Co[redacted]l From: [redacted]
Re: 66F-HQ-C136[redacted]0, 03/09/2004

b2
b7E

LEAD(s):

Set Lead 1: (Info)

ALL RECEIVING OFFICES

Read and clear.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/15/2004

To: International Operations **Attn:** IO2,
General Counsel **Attn:** , ILU

From:
Contact:

Approved By:

Drafted By:

Case ID #: 66F-HQ-C1364260 (Pending)
66F-HQ-C1384970 (Pending)

Title: USA PATRIOT ACT;
SUNSET PROVISIONS

Synopsis: Response to lead on use of the USA Patriot Act.

Reference: 66F-HQ-C1364260 Serial 5
66F-HQ-C1384970 Serial 7564

Details: is a conduit of information from Field Offices and FBIHQ to liaison; however, assumes that a number of investigative leads were generated for this office because of the provisions of the USA Patriot Act. hopes that Field Offices are responding to this request so that OGC is able to provide the necessary justification to Congress.

To: International Operations From: [redacted] b2 b7E
Re: 66F-HQ-C1364260, 03/15/2004

LEAD(s):

Set Lead 1: (Info)

ALL RECEIVING OFFICES

Read and clear.

I:\[redacted]\PATRIOT.EC b6 b7C

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 03/19/2004 **Date:** 03/17/2004

To: Office of General Counsel **Attn:** Investigative Law Unit
[redacted]
Room 7326

From: [redacted]
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted] ths

Case ID #: 66F-HQ-C1364260 -17
66F-HQ-1384970 -8049
66F-[redacted]-28229 -8

Title: USA PATRIOT ACT
SUNSET PROVISIONS

b6
b7C
b2
b7E
b6
b7C
b2
b7E

Synopsis: Review of [redacted] USA PATRIOT Act subfiles previously established to document the effective use of these tools in anticipation of the 12/31/2005 sunset.

Reference: 66F-HQ-C1364260 Serial 5

Details: On 03/26/2003, via EC to all employees, [redacted] established USA PATRIOT Act subfiles to document the effective use of these provisions which are scheduled to sunset on 12/31/2005.

b2
b7E

The USA PATRIOT Act provisions subject to sunset concern, voice mail, nationwide search warrants for e-mail, information sharing, voluntary disclosure by ISP, immunity from civil liability, expanded predicates for Title III, roving FISA surveillance, new standard for FISA Pen/Trap, new standard for business records under FISA, changes to "primary purpose" standard in FISA, monitoring communications of computer trespassers, and certification forms submitted to FinCen for terrorism and money laundering investigations.

[redacted] periodically sends out e-mails to all personnel as a reminder that the usage of these provisions must be tracked and documented in the appropriate subfiles.

b1
b2
b7E

[redacted] (S) The results of

To: Office of General Counsel From: [redacted] b2 b7E
Re: 66F-HQ-C1364[redacted]0, 03/17/2004

these [redacted] requests enabled investigators to identify previously unknown [redacted] associated with captioned subjects. Additionally, with respect to one of these b2 b7E

[redacted]

To: Office of General Counsel From: [redacted]
Re: 66F-HQ-C1364[illegible]0, 03/17/2004

b2
b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Information only.

♦♦

~~SECRET~~

(Rev. 01-31-2003)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 03/19/2004 **Date:** 03/18/2004 b6

To: General Counsel **Attn:** Investigative Law Unit b7C
[redacted] Rm. 7326

From: [redacted] b2
Squad 1 b7E b2
Contact: CDC [redacted] b6

Approved By: [redacted] b6

Drafted By: [redacted] jpm b7C

DATE: 09-09-2005 b7C
CLASSIFIED BY 65179 DMH/KJ
REASON: 1.4 (c)
DECLASSIFY ON: 09-09-2030

Case ID #: 66F-HQ-C1364260 (Pending) -19
66F-HQ-C1384970 (Pending) .8113
66-[redacted]-63323 (Pending) .43

05-CV-0845

b2
b7E

Title: USA PATRIOT ACT
SUNSET PROVISIONS
[redacted] DIVISION STATISTICS

b2
b7E

Synopsis: Provide OGC with requested information regarding [redacted] use of Patriot Act Provisions.

Reference: 66F-HQ-C1364260 Serial 5

b2
b7E

Details: Referenced serial requested statistical information from [redacted] regarding use of USA Patriot Act provisions. The requested information from [redacted] IT and FCI investigations is as follows:

STATISTICS

Technique	Times Used
[redacted]	(S)

b1
b2
b7E

~~SECRET~~

To: General Counsel From: [redacted] b2 b7E
Re: 66F-HQ-C1364260, 03/18/2004

[redacted] (S)

b1
b2
b7E

[redacted] (S)

b1
b2
b7E

To: General Counsel From: [redacted]
Re: 66F-HQ-C1364260, 03/18/2004

b2
b7C

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

As requested in referenced serial. Read and clear.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/17/2004

To: General Counsel **Attn:** Investigative Law Unit
[redacted]
Room 7236

From: [redacted]
SAC
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted] amd

Case ID #: 66F-HQ-C1364260-20

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: [redacted] examples of the use of USA Patriot Act sunset provisions to achieve investigative goals.

Details: The following is set forth regarding use of investigative tools created by the Patriot Act:

1.) Intercepting communications of computer trespassers.

[redacted]

[redacted]

[redacted]

b2
b7E

[redacted] b7A

[redacted] b7A

2.) Changes to "Primary Purpose" Standard for FISA.

[redacted] b6 b7A b7C

[redacted] b6 b7A b7C

[redacted] The changes to the FISA Sections 218 and 504 enabled criminal investigators and prosecutors to review and present

b2
b7E
b6
b7A
b7C

material leading to [redacted]

[redacted] The material support portion of the investigation is ongoing.

b6
b7A
b7C

3.) Information Sharing

The cooperation between other Government Agencies within the Intelligence Community (IC) and the FBI has resulted in significant improvements in the conduct of everyone's mission. [redacted] has prepared FISA requests in two separate matters based on information from the IC. Three potential compromises in ongoing foreign intelligence investigations were averted through the timely sharing of information. Numerous IT cases benefitted from the receipt of intelligence from the IC and vice versa. Follow-up investigations have been coordinated with the IC when FBI - IT subjects have departed the U.S., whether the departure was voluntary or not. Numerous IIRs disseminating foreign intelligence and/or positive terrorism intelligence have been generated.

b2
b7E

♦♦

~~SECRET~~

(Rev. 01-31-2003)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 08-26-2005
CLASSIFIED BY 65179 DMH/KJ/05-cv00845
REASON: 1.4 (c)
DECLASSIFY ON: 08-26-2030

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/18/2004

To: FBIHQ **Attn:** Office of General Counsel
Investigative Law Unit
[redacted]
Room 7326

b6
b7C
b2
b7E

From: [redacted]
11A
Contact: ADC [redacted] Ext. [redacted]

b2
b6
b7C

Approved By: [redacted]

Drafted By: [redacted] :jaw

b6
b7C

Case ID #: 66F-HQ-C1364260 (Pending)
66F-HQ-C1384970 (Pending)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: [redacted] response to Patriot Act survey.

b2
b7E

Reference: 66F-HQ-C1364260 Serial 5
66F-HQ-C1384970 Serial 7564

Details: A canvas was conducted of all counterintelligence and counterterrorism squads regarding the provisions of the USA Patriot Act which are subject to the sunset provisions. The following details the results:

Voice Mail (Section 209) - [redacted] (S)

b1
b2
b7E

is a valuable tool. In an emergency situation obtaining a search warrant would be much faster and less complicated than obtaining an emergency Title III. [redacted] (S)

Nationwide Search Warrants for E-mail (Section 220) - The [redacted] (C) (S)

b1
b2
b7E

this is a crucial provision for [redacted] Prior to the USA Patriot Act a great deal of manpower was used obtaining

~~SECRET~~

b2
b7E

search warrants for other divisions for e-mail carriers which are located in the [redacted] still spends a great deal of time serving process for other divisions, however, it is nothing like the days after 9/11 when SAs were required to draft and swear to affidavits for all the other divisions.

Voluntary Disclosures (Section 212) - [redacted] (S) This provision is essential to [redacted] for the same reasons as stated above. Due to the number of communication carriers in the division, it is imperative that we are able to request this type of information from communications carriers in an emergency situation. [redacted] (S)

b1
b2
b7E

Information Sharing (Section 203(b) &(d)) - [redacted] A considerable amount of Grand Jury material has been shared, but to this date [redacted] investigations have generated information pertinent to any CI or CT investigations. However, due to the new 315 classification and the removal of the wall between the criminal and intelligence worlds, it is imperative that information be permitted to flow in both directions.

Intercepting Communications of Computer Trespassers (Section 217) - [redacted] Although, most of [redacted] computer hacking cases have [redacted] it is anticipated that it will occur in the near future. (S)

b1
b2
b7E

Expanded Predicates for Title III (Sections 201 & 202) - [redacted] It is very important that all tools be made available in the fight against terrorism. At this time, FISA is primarily being used to obtain ELSUR on [redacted] IT subjects, however, it is crucial that the FBI have the ability to neutralize terrorists where the danger they pose outweighs the value of the intelligence that we maybe able to collect. Title III is an excellent investigative tool that should be available in the fight against terrorism. (S)

b1
b2
b7E

Roving FISA Surveillance (Section 206) - [redacted] It was necessary to cover a subject's move [redacted] (C) (S)

b1
b2
b7E

[redacted] (S) b1

New Standard for FISA Pen/Trap (Section 214) - [redacted] (S)

This technique has provided contacts for potential assets and has aided in developing the subject's personal profile. However, this is a under utilized technique due to the length of time it takes to obtain, most agents wait and request a FISA [redacted] (S) b1 b2 b7E

Changes to "Primary Purpose" Standard for FISA (Section 218) - [redacted] (S) b1

However, it is arguable that this provision has aided in obtaining the majority of IT FISAs. It is necessary to maintain this provision in order to continue investigating counterterrorism under the 315 classification.

New Standard for Business Records under FISA (Section 215) - [redacted] (S) b1 b2 b7E

♦♦

~~SECRET~~

(Rev. 01-31-2003)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/18/2004

To: General Counsel **Attn:** Investigative Law Unit b6
Room 7326 b7C

From: [redacted] b2
Legal Unit b7E
Contact: CDC [redacted] [redacted] b2
b6

Approved By: [redacted] b6

Drafted By: [redacted] b7C

DATE: 09-09-2005
CLASSIFIED BY 65179 DMH/JK
REASON: 1.4 (c)
DECLASSIFY ON: 09-09-2030 b7C

05-CV-0845

Case ID #: 66F-HQ-C1364260-12 (Pending)
66F-HQ-C1384970-8135

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: Summary of benefits [redacted] has received from various provisions of the USA PATRIOT Act. b2

Details: The following provides statistics, examples, and brief narratives summarizing some of the benefits the [redacted] has received from various provisions of the USA PATRIOT Act: b7E

***Nationwide Search Warrants for E-mail and Associated Records* - Section 220 of the Act. See 18 U.S.C. § 2703.**

This technique has been used frequently for e-mail records. Without it service would have been much more time consuming and less successful.

[redacted] During this investigation, FISA coverage was conducted for approximately one year. A significant part of the coverage included several e-mail accounts [redacted] Part of the success and ease of initiating this coverage hinged on this provision. Each of the e-mail providers were located in a different part of the country. If this provision were not in place, this coverage, which was deemed urgent at the time of initiation, would have been dramatically hindered and crucial intelligence lost or delayed. b7A b2 b7E

***Information Sharing* - Section 203(b) & (d) of the Act.**

~~SECRET~~

Generally speaking we are now able to discuss our cases with other agencies much more freely. This has streamlined and greatly facilitated our investigations. b2 b7E

1990 [redacted] 66215 (Closed) [redacted] b1 (S)

[redacted] Investigation revealed subject to be a con-man who was primarily raising money for his own personal benefit. However, investigation also revealed subject was engaged in various criminal activities. Sections 203(b) and 203(d) were utilized in allowing information from the criminal case to be shared with the intelligence investigator. The intelligence investigation produced an enormous amount of intelligence, including information received from several foreign intelligence services. Section 218 and Section 504 were utilized to share the pertinent parts of that intelligence with the criminal investigator, as well as the federal prosecutors. Without all three of these provisions, both the criminal and intelligence investigators would have been conducting simultaneous and parallel investigations, without the ability to have a complete picture of the subject, thereby, resulting in lengthy and duplicative investigative efforts. As a direct result of these enabling provisions of the USA Patriot Act, the subject was ultimately convicted on the criminal charges and, consequently, deported from the United States. However, prior to subject's deportation, subject provided a tremendous amount of valuable information which has been used in approximately a dozen [redacted] investigations alone, plus an additional half dozen cases in other divisions across the United States. b2 b7E

[redacted] The information sharing portion of the act has impacted the effectiveness of the [redacted] which participated in the referenced case which involved threat mailings. The ability to share information has enriched FBI liaison with State, Local and other Federal agencies, resulting in better relationships. b2 b7E

When events broke in this case requiring JTTF response, the ability to organize an action plan among the agencies was greatly enhanced. A level of trust resonated among investigators which resulted in a style of teamwork imperative in the first few days after the threat mailings. The ability to share information relieved the case agent from being overwhelmed, and allowed for a much more effective investigation.

[redacted] This is an investigation of an increasingly [redacted] organization, with its leaders in the United States advocating and preparing for violence. In recent years, radicals have infiltrated the group's leadership in the US with several key members advocating violence. [redacted] b7A

[redacted] this threat would be difficult to combat given the respect and legal protections the group enjoys in the US and overseas. b7A

Information sharing with [redacted] and [redacted] is essential to identifying the subjects' associates, travel, and activities in support of this organization.

[redacted] In this case, we opened a parallel investigation on the criminal side. Subpoenas were used for financial information and NSLs for toll records. Previously, we would have had difficulty sharing the NSL results with the criminal side. When we obtained pertinent information from the criminal side, we had to send an NSL for the same information in order to use it for the intelligence side, duplicating voluminous work on the part of the Bureau and the service provider. Also, the criminal case agent would not have been apprized of significant developments on the intelligence side of the case. Recently, [redacted] b7A The criminal case agent would not have been in a position to assist us if he had not been fully briefed in on the case. Due to the criminal agent's work, a valuable source was successfully recruited.

Due to the complexities inherent in this [redacted] terrorism investigation, this case has been a joint effort between the following agencies: FBI [redacted] b7A b2

[redacted] These cases involve [redacted] b7A The purpose of the investigation is to determine if these businesses and/or their owners/employees are forwarding funds overseas in support of terrorist activities.

The Information Sharing sections of the USA Patriot Act have been critical in that the investigation is being conducted [redacted] Information sharing between the FBI and these agencies has been instrumental in identifying subjects, conducting surveillance and obtaining various records. Due to these Patriot Act provisions, intelligence information can be shared which greatly affects the utilization of resources and the focus of the case. b7A

To: General Counsel From: [redacted] b2 b7E
Re: 66F-HQ-C1364260 03/18/2004

b1 b7A

[redacted] (S)

[redacted] This investigation was initiated based on information sharing between intelligence agencies, [redacted] and FBI. This aspect of intelligence sharing between agencies in the intelligence community has been a tremendous asset in this investigation, particularly with [redacted] b2 b7A

At the outset of this investigation, a parallel criminal investigation was initiated, which at the time was still under the mandate of the previous guidelines which forbid information sharing between intelligence and criminal investigations of the same subject. This was an excellent opportunity to witness the difference between the guidelines when a "wall" existed and the new guidelines where the "wall" was removed between criminal and intelligence investigations. Under the criminal investigation, subpoenas were issued for toll records and financial information. Since this was during the "wall" period, the criminal agent and the intelligence agent could not and would not be in the same room while there was information received as a result of the subpoenas. Likewise, when intelligence information was received from a linked FISA investigation, the criminal agent would remain completely unaware of the new intelligence which could aid in the direction of the criminal investigation. The AUSA assigned to the investigation was particularly uncomfortable with the investigation for fear of violating the guidelines of influencing the intelligence investigation. This placed the AUSA in a precarious position: needing to know all the information from both aspects of the investigation and yet not wanting to mistakenly report information from the criminal agent to the intelligence agent and vice versa. The "wall" procedures hindered the investigation of terrorism cases tremendously.

After the "wall" was removed, the difference in the investigation was obvious and significant. Meetings between the USA, AUSA, intelligence agents, criminal agents were regular and productive. This allowed a team aspect to investigations between the USA's office and the agents in the field.

Practical aspects of information sharing involved less repetitive effort duplicating information. An example of this would be information from subpoenas and National Security Letters

(NSL). Before, the criminal investigation could not have any information gathered as a result of a NSL and likewise with intelligence investigations having information gathered from a subpoena. This required two documents to be issued per one piece of information.

Since the implementation of the new provisions, information from this investigation has been shared with several other FBI field offices which has resulted in an expanded picture of potential terrorist activities within the United States. This provision is crucial to the ongoing effort against terrorist threats to the United States.

New Standard for FISA Pen/Trap **- Section 214 of the Act.**

[redacted] b7A

accounts.

[redacted] b2 b7E b7A

[redacted] The old standard of "specific and articulable facts" that the line was used by an agent of a foreign power was changed to a relevance to terrorism standard. [redacted]

[redacted] b7A b2 b7E

Changes to "Primary Purpose" Standard for FISA -
Section 218. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials.

b2
b7E

281F-[redacted]66686: Information was shared from the case agent in the above referenced 199Q[redacted]66215 investigation under Section 218 and Section 504 with the criminal investigator and federal prosecutors to convict one of the subjects of this investigation. Having the criminal side fully apprized of all of the intelligence was of great benefit as this helped in the coordination of surveillance and the interviews of certain individuals connected to this investigation. After completing his sentence in federal prison, this particular subject of this criminal investigation will also be deported from the United States. All of this was facilitated by the sharing provisions under the USA Patriot Act.

b1
b7A
b6
b7C

[redacted](S) Section 218 has enabled the intelligence received from a foriegn intelligence/security agency regarding subject to be shared with federal prosecutors both in two Divisions. This is an ongoing investigation.

[redacted] This intelligence investigation was opened based solely on information provided by the subject of above referenced closed 199Q-[redacted]66215 investigation. This information alleged the

b2
b7E

[redacted] Through the coordinated efforts of various divisions and resident agencies, information was received from several foreign intelligence services regarding subject. This intelligence included information about [redacted]

b7A
b6
b7C

As a direct result of being able to share this intelligence under Section 218 and Section 504 of the USA Patriot Act with other agencies involved with this investigation, [redacted]

[redacted] Without these referenced provisions of the USA Patriot Act, this coordinated investigative effort between a multitude of various federal, state, local, and international law enforcement

agencies would have been much more difficult with possibly a much different result.

[redacted] The changing of the FISA standard from a "primary purpose" to "a significant purpose" has had a dramatic impact on terrorism cases and this particular investigation would not have been possible without this change. This investigation centered on [redacted] The FISA coverage of the subject was initiated after intelligence indicated that [redacted] This information would fall primarily in the criminal aspect of a terrorist attack and negate the "primary purpose" standard for FISA coverage since the purpose was not to gather intelligence but to use the criminal justice system to stop a terrorist attack. As a result of the changing standard, FISA coverage was initiated and further information was gathered to accurately assess the threat. b7A

***New Standard for Business Records under FISA* - Section 215.**

[redacted] We have obtained [redacted] NSLs for records from a [redacted] b7A b2 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Read and clear.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

Precedence: PRIORITY **Date:** 03/18/2004

To: General Counsel **Attn:** Investigative Law Unit
attn: [redacted] Rm 7326

From: [redacted]
CDC
Contact: SSA [redacted]

b2
b7E
b2
b6
b7C

Approved By: [redacted]

Drafted By: [redacted] mrs

b6
b7C

Case ID #: 66F-HQ-C1364260-24 (Pending)
66F-HQ-C1384970-8144

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: Providing OGC, ILU with information concerning provisions of the Patriot Act subject to the Sunset Provision.

Reference: 66F-HQ-1085160 Serial 57
66F-HQ-C1364260 Serial 1

Details: A survey conducted among the Supervisory Special Agents in the [redacted] division indicate that, by far, the most important and utilized provision of the Patriot Act has been the delegated authority to the field to utilize NSLs in appropriate investigations. Also the ability to share information between intelligence investigations and criminal investigations has proven invaluable.

b2
b7E

As to the specific provisions of the Patriot Act subject to sunset provisions [redacted] has no anecdotal or statistical information to provide ILU.

To: General Counsel From: [redacted]
Re: 66F-HQ-C13642[redacted] 03/18/2004

b2
b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT INVESTIGATIVE LAW UNIT

Read and clear.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

55

Precedence: ROUTINE **Date:** 03/16/2004

To: General Counsel **Attn:** [redacted]
Investigative Law Unit

From: [redacted]
Legal Unit
Contact: SSA [redacted], CDC, [redacted]

Approved By: [redacted]

Drafted By: [redacted]:dlk

Case ID #: 66F-HQ-C1364260-25
66F-HQ-C1384970-8151
66F-CI-A71844-133

Title: USA PATRIOT ACT
SUNSET PROVISIONS

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-09-2005 BY 65179 DMH/KM

05-CV-0845

Synopsis: To report the [redacted] use of USA Patriot Act sunset provisions as requested in referenced EC.

Reference: 66F-HQ-C1364260 Serial 5

Details: To report [redacted] positive use of investigative tools provided by provisions of the Patriot Act, subject to a legislative "sunset" clause.

Information Sharing (Section 203) March 2004. Gave authority to Joint Terrorism Task Force agents to [redacted] of suspected AQ fund raiser. May provide circumstantial evidence of suspect materially supporting terrorism.

[redacted]

Use of Federal Grand Jury Subpoenas.

Roving FISA Surveillance - Section 206 - The [redacted] RA Joint Terrorism Task Force [redacted]

[redacted]

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C13642[redacted], 03/16/2004 b7E

[redacted] b2
b7E

*New Standard for FISA Pen/Trap (*Section 214) - This technique has been utilized multiple times within our district. Information from this technique has led to discovery of other suspects. Other investigations are ongoing. This investigative tool has been used with electronic communications [redacted] b2
b7E

Changes to "Primary Purpose" Standard for FISA(Section 218) - amended under Section 504 - coordination w/ law enforcement under FISA. - FISA information is shared routinely with all cleared personnel involved in the Joint Terrorism Task Force.

New Standard for Business Records under FISA (Section 215) - the [redacted] b2
b7E

The following sections are not listed in the referenced EC, but are included due to their value to investigators:

Scope of subpoenas for records of electronic communications (Section 210) - the [redacted] b2
routinely uses Grand Jury Subpoenas to cover leads and further investigate b7E
suspects in Joint Terrorism cases. The [redacted] processes approximately 10 National Security letters per week, covering ECPA, RFPA and FCRA.

Modification of authorities relating to use of pen registers and trap and trace devices (Section 216)

b2
November 2003. Pen's initiated on [redacted] b7E
[redacted] Investigation by Joint Terrorism Task Force continuing.

Defendant [redacted] is charged in a federal criminal complaint in [redacted] with Unlawful Flight to Avoid Prosecution (UFAP). He was charged by local authorities with trafficking in marijuana, possession of marijuana, and conspiracy. There is also a federal investigation open for making threatening communications. [redacted] b2
b7E
b6
b7C
[redacted] -Louisville, Ky., and [redacted] -Dallas, Texas.) The PATRIOT Act allowed us to obtain the pen/trap orders from a magistrate judge in our district for [redacted]. This saved a

b2
b7E

b6
b7C

great deal of time and meant that we did not have to involve AUSAs from two other districts. [redacted] remains a fugitive.

(S)

[redacted]

b1
b2
b7E
b6
b7C
b7A

To: General Counsel From: [redacted]
Re: 66F-HQ-C13642[redacted], 03/16/2004

b2
b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Read and clear.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 03/19/2004 **Date:** 03/17/2004

To: General Counsel **Attn:** ILU, Room 7326
Attention: [redacted] b6 b7C

From: [redacted]
Squad 21
Contact: SSA [redacted] b2 b7E [redacted] b2 b6 b7C

Approved By: [redacted]

Drafted By: [redacted] b6 b7C

Case ID #: 66F-HQ-C1364260 ;26 .

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: To provide a brief narrative summarizing [redacted] use of several authorities implemented by the USA Patriot Act which are subject to sunset provisions. Referenced lead covered. b2 b7E

Reference: 66F-HQ-C1364260 Serial 5

Details: Above referenced communication requested offices to provide the Investigative Law Unit (ILU), Office of the General Counsel (OGC), with "statistics, good examples or anecdotes, or at the very least, a brief narrative summarizing the benefits the office has received from the provisions...."

To that end, [redacted] provides the following information: b2 b7E

1. Voice Mail - Section 209 of the Act permits law enforcement to obtain a search warrant or court order for voice mail messages maintained by a communications provider under 18 USC 2510 or 2703.

[redacted] (S) Although this investigative technique [redacted] it is a valuable tool. In an emergency situation obtaining a search warrant would be much faster and less complicated than obtaining an emergency Title III. b1 b2 b7E

To: General Counsel From: [redacted] b2 b7E
Re: 66F-HQ-C13642[redacted], 03/17/2004

b1 b2 b7E

2. Nationwide Search Warrants for email - Section 220 of the Act permits the issuance of search warrants with nationwide jurisdiction to an electronic communications service provider under 18 USC 2703.

[redacted] (S)

3. Voluntary Disclosures by ISPs - Section 212 of the Act permits communications providers to voluntarily disclose the contents of communications to protect life or limb or their rights or property.

b1 b2 b7E

[redacted] (S)

4. Information Sharing - Sections 203(b) and (d) of the Act permit the sharing of information between criminal and intelligence investigations.

b1 b2 b7E

[redacted] (S)

FISA coverage on a close associate provided invaluable information on the first subject, in particular the timing of his arrest, as he was in the process of leaving the country on extremely short notice (the arrest was made at the airport.) The IT subject ultimately pleaded guilty to a White Collar Criminal charge, was denaturalized, and deported out of the country. [redacted] can provide a more detailed, classified, case review upon request.) b2 b7E

5. Intercepting Communications of Computer Trespassers - Section 217 of the Act permits a computer owner/operator to provide consent for law enforcement to monitor the activities of a computer trespasser.

b1 b2 b7E

[redacted] (S)

6. Expanded Title III Predicates - Sections 201 and 202 of the Act permit the use of court authorized electronic surveillance (i.e. a Title III) in investigations involving chemical weapons (18 USC 229), terrorism (18 USC 2332a, 2332b, 2332d, 2339A and 2339B) or computer fraud and abuse (18 USC 1030.)

b1 b2 b7E

[redacted] (S)

To: General Counsel From: [redacted] b2 b7E
Re: 66F-HQ-C13642[redacted], 03/17/2004

b1 b2 b7E

7. **Roving FISA Surveillance** - Section 206 of the Act permits roving surveillance where the target is attempting to thwart electronic surveillance.

[redacted] (S) However, [redacted] anticipates the increased use of this important authority to combat the increasingly sophisticated trade craft employed by IT and FCI subjects. b2 b7E

8. **New Standard for FISA Pen/Trap** - Section 214 of the Act authorizes a FISA Order for a pen register or trap/trace based upon the standard that such is relevant to the investigation. b1 b2 b7E

[redacted] (S)

9. **Changes to the "Primary Purpose" Standard for FISA Court Orders** - Section 218 of the Act authorizes the issuance of a FISA Court Order where foreign intelligence gathering is a "significant purpose" rather than the "primary purpose" for the Order.

This provision along with the information sharing provisions are the cornerstones of the PATRIOT ACT. [redacted] has had great success in the sharing of FISA information to assist members of the Intelligence Community (IC) as well as other criminal agencies, and the US Attorneys Office. In one particularly noteworthy example, the subject of a two year long FISA was subsequently arrested on a weapons charge stemming from an incident that happened prior to 9/11/01. In preparation for the trial, [redacted] coordinated closely with the AUSA's office to identify potentially useful FISA cuts in preparation for a trial. While the subject ultimately pled guilty prior to trial, significant time and resources were committed to reviewing the FISA cuts in preparation and coordinating a unified strategy between the [redacted] the AUSA's office and the arresting agency. [redacted] can provide a more detailed, classified, case review upon request.) b2 b7E

10. **New Standard for Business Records Under FISA** - Section 215 of the Act permits the issuance of a FISA Court Order for record production where the information is relevant to an investigation.

[redacted] (S) Again, however, [redacted] considers this authority to be extremely valuable, in particular when the use of a National Security Letter (NSL) is not authorized or appropriate. b1 b2 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Read and Clear.

♦♦

~~SECRET~~

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

55

Precedence: DEADLINE 03/19/2004 **Date:** 03/18/2004

To: General Counsel **Attn:** Investigative Law Unit
[redacted]

b2
b7E b6
b7C

From: [redacted]
Squad 1
Contact: CDC [redacted]

Approved By: [redacted]

Drafted By: [redacted] 27 b6
b7C

Case ID #: 66F-HQ-C1364260 (None)
66F-HQ-C1384970 (None)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: To provide a brief narrative summarizing benefits [redacted] has received from specified provisions of USA PATRIOT Act. b2
b7E

Reference: 66F-HQ-C1364260 Serial 5
66F-HQ-C1384970 Serial 7564

Details: Field offices were requested to provide OGC with statistics, good examples or anecdotes, or at a minimum, a brief narrative summarizing the benefits the office has received from the specified sunset provisions of the USA PATRIOT Act. Listed below are the specific provisions scheduled to sunset with brief commentary regarding use by the [redacted] b2
b7E

b1
b2
b7E

Voice Mail - Section 209:

[redacted] (S)

b1
b2
b7E

Nationwide Search Warrants for E-Mail and Associated Records - Section 220:

[redacted] (S)

Voluntary Disclosures - Section 212:

[redacted] (S)

b1
b2
b7E

~~SECRET~~

To: General Counsel From: [redacted] b2 b7E
Re: 66F-HQ-C1364260, 03/18/2004

Information Sharing - Section 203(b) and (d):

[redacted] b1 (S)

Some but not all specific case examples would include the following: (S)

1) In 315Q-[redacted]56983, information was obtained from a criminal case CW regarding the subject of a foreign intelligence investigation who was suspected of planning a terrorist act. Sharing of intelligence information developed regarding the subject led to the interception, arrest and anticipated deportation of the subject. b2 b7E

2) [redacted] intelligence information was shared [redacted] b7A

3) In [redacted] pen register information obtained through a traditional criminal court Order directly supported a FISA application which has been prepared and forwarded to FBIHQ. b7A

4) In [redacted] an intelligence investigation, information was developed regarding [redacted] This information was provided to [redacted]

Expanded Predicates for Title III - Sections 201 and 202:

[redacted] b1 (S) b2 b7E

Roving FISA Surveillance - Section 206:

b1 b2 b7E [redacted] (S)

New Standard for FISA Pen/Trap - Section 214:

[redacted] b1 (S) b2 b7E

Changes to "Primary Purpose" Standard for FISA - Section 218:

b1 b2 b7E [redacted] (S)

In drafting these applications information obtained through traditional criminal investigative methods has been shared and incorporated into the application. The FISA application which is pending before OIPR was developed through file number 315N-[redacted]6807. b2 b7E

~~SECRET~~

To: General Counsel From: [redacted] b2 b7E
Re: 66F-HQ-C1364260, 03/18/2004

New Standard for Business Records under FISA - Section 215:

[redacted] (S) b1 b2 b7E

~~SECRET~~

To: General Counsel From: [redacted]
Re: 66F-HQ-C1364260, 03/18/2004

b2
b7E

LEAD(s):

Set Lead 1: (Discretionary)

GENERAL COUNSEL

AT WASHINGTON, DC

Read and disseminate as appropriate.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/19/2004 b6 b7C

To: General Counsel **Attn:** [redacted] ILU, Rm. 7326

From: [redacted] b2

Contact: [redacted] b7E b2

Approved By: [redacted] b6 b7C

Drafted By: [redacted] b6 b7C

Case ID #: 66F-HQ-C1364260-30
66F-HQ-C1384970-862

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: This EC contains a couple of anecdotes regarding the benefits conferred on [redacted] investigations by the Patriot Act.

Reference: 66F-HQ-C1364260 Serial 5

Details: While attempting to gather information for a full response to the referenced serial, [redacted] could not locate reliable data on the impact that lapsing Patriot Act provisions have had on [redacted] investigations, but [redacted] is happy to report that Agents provided a couple of interesting anecdotes. b2 b7E

[redacted] b2 b6 b7A b7C b7E

[redacted] This vital information led to the issuance of 8 indictments and the seizure of numerous bank and financial accounts totaling nearly $600,000.00.

[redacted] Since the enactment of Section 504 of the Patriot Act, Agents operating FISAs have been able to use intelligence generated therefrom to assist criminal Agents and criminal AUSAs in prosecuting the [redacted] case. Foreign intelligence information, e.g. travel information, collected through use of FISC-authorized electronic surveillance in the b2 b7E

cases involving [redacted], and [redacted] has aided the criminal investigations and subsequent prosecutions of these subjects. b7A b6 b7C

If [redacted] learns of other relevant anecdotes, it will provide them to the Investigative Law Unit immediately. b2 b7E

♦♦

~~SECRET~~

(Rev. 01-31-2003)

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

DATE: 08-29-2005
CLASSIFIED BY 65179 DMH/KJ/05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 08-29-2030

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

b7

Precedence: ROUTINE **Date:** 03/19/2004

To: General Counsel **Attn:** Investigative Law Unit b6
[redacted] b7C
Room 7326

From: [redacted] b2
Squad I - Chief Division Counsel (CDC) b7E
Contact: [redacted] - [redacted] b2

Approved By: [redacted] b6

Drafted By: [redacted] jbk b7C

Case ID #: (U) 66F-HQ-C1364260 (Pending) -31 b7A
(U) [redacted] (Pending) -211

Title: (U) USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: (U) This communication reports examples of the [redacted] use of portions of the USA Patriot Act which will sunset in 2005. b2 b7E

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Administrative: (U) Reference is made to the 02/27/2004 electronic communication (or EC) of the Office of the General Counsel.

Details: (U) The following are examples of the [redacted] use of portions of the USA Patriot Act which will sunset in 2005: b2 b7E

(U) Nationwide Search Warrants for Email and Associated Records

~~(S)~~ [redacted]

(U) Information Sharing

b1
b2
b7E

~~SECRET~~

~~SECRET~~

SECRET

To: General Counsel From: [redacted] b2 b7E
Re: (U) 66F-HQ-C1364260, 03/19/2004

b1 b2 b7E

(S) The referenced EC requested specific examples relating to Sections 203(b) and (d) of the USA Patriot Act. [redacted] (S) But the following is offered:

b1 b2 b7E

(S) [redacted] (S) Relevant information developed in the criminal investigations was shared with those in charge of the international terrorism investigations, and vice versa.

(U) (S) The [redacted] Joint Terrorism Task Force (JTTF) established liaison with the U.S. Department of Education and the IRS - Treasury Inspector General for Tax Administration.

(U) (S) The Department of Education offered to share information regarding foreign students under the provisions of the Patriot Act, provided that the requesting JTTF member attests that terrorism may be involved. Information available includes extensive background data concerning students who have requested grants. To date, two requests have been submitted to the Department of Education. These requests are pending. b2 b7E

(U) (S) The [redacted] JTTF received a similar offer from IRS - Treasury Inspector General for Tax Administration to share information regarding potential terrorist subjects. Information includes a query of a threat database maintained regarding individuals who have expressed anti-government sentiment, specifically tax protesters. Information to be shared is limited to whether an individual posed a possible threat, or did not pay taxes based on anti-government beliefs. This information is most useful regarding domestic terrorism cases. To date, two requests were been submitted, but both yielded negative results.

(U) Roving FISA Surveillance

[redacted] (S)

(U) New Standard for FISA Pen/Trap

b1 b2 b7E

SECRET

To: General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/19/2004 b7E

[redacted] (S) b1 b2 b7E

(U) Changes to "Primary Purpose" Standard for FISA

[redacted] (S) b1 b2 b7E

SECRET

To: General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/19/2004 b7E

LEAD(s):

Set Lead 1: (Discretionary)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) For information and discretionary action.

♦♦

SECRET

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/19/2004

To: General Counsel **Attn:** [redacted]
Investigative Law Unit
Room 7326

International Operations **Attn:** SSA [redacted] IOU-I

From: [redacted]
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted] H:mhr

Case ID #: 66F-HQ-C1364260 (Pending)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 08-15-2005
CLASSIFIED BY 65179 DMH/KJ/05-cv-0845
REASON: 1.4 (d)
DECLASSIFY ON: 08-15-2030

Synopsis: To provide examples of use of Patriot Act provisions. Lead covered at [redacted]

Reference: 66F-HQ-C1364260 Serial 5

Details: [redacted] has utilized provisions of the Patriot Act as it relates to e-mail communications [redacted] (S) [redacted] These cases involved the utilization of Hotmail and/or Yahoo accounts by Subjects for the purpose of communicating with victims or the families of victims.

[redacted] contacted the U.S. Department of Justice (DOJ) Office of International Affairs (OIA) and Computer Crime & Intellectual Property Section (CCIPS). [redacted] 2703(f) preservation letters were submitted, subsequently 2703(d) letters were drafted and submitted by DOJ. [redacted] involved the utilization of Hotmail e-mail for communication between a fugitive in an [redacted] homicide investigation. [redacted] both Hotmail and Yahoo were utilized in an attempt to extort funds from the Argentine subsidiary of a large United States accounting and financial services firm.

[redacted] a kidnaping was resolved, and a victim rescued, as a result of the voluntary release of non-content Hotmail e-mail data by MSN. In this investigation, MSN

~~SECRET~~

To: General Couns[redacted] From: [redacted]
Re: 66F-HQ-C1364260, 03/19/2004

b1
b2
b7E

[redacted] based attorneys worked in conjunction with [redacted]

[redacted] (S)

To: General Counsel From: [redacted]
Re: 66F-HQ-C1364260, 03/19/2004

b2
b7E

LEAD(s):

Set Lead 1: (Info)

ALL RECEIVING OFFICES

For information.

◆◆

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 03/19/2004 **Date:** 03/18/2004

To: General Counsel **Attn:** ILU, Room 7326

b6

From: b2 b7C b2

Contact: b7E b6

DATE: 09-12-2005
CLASSIFIED BY 65179 DMH/KJ b7C
REASON: 1.4 (C)
DECLASSIFY ON: 09-12-2030 b6

Approved By: b7C

Drafted By:

05-CV-0845

Case ID #: 66F-HQ-C1364260-33 (Pending)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: Response to OGC request for information on Patriot Act utilization.

Reference: 66F-HQ-C1364260 Serial 5

Details: The b2 has had the opportunity to utilize various Patriot Act provisions, most frequently, by taking advantage of the new legal standards related to FISA techniques. b7E b1

b2

b7E

(S)

The new information sharing capabilities has allowed the b2 to share important information with the intelligence community, most notably in the following cases: b7E

b1

(S) b7A

b6

b7C

(S)

b1

b7A

b6

b7C

~~SECRET~~

KMS07803.EC

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364260 03/18/2004 b7E

[redacted] (S) b1 b6 b7C

The Patriot Act has also allowed information sharing between the criminal investigation and intelligence investigation [redacted] (S) b1 b7A

A nationwide search warrant for electronic communication records was utilized in the [redacted] (S) b6 b7C investigation, providing for more efficient use of investigative resources.

b1
b6
b7C

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364260 03/18/2004 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Read and clear.

◆◆

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

Precedence: ROUTINE **Date:** 03/19/2004

To: General Counsel **Attn:** [redacted] ILU
Rm. 7326

From: [redacted]
Squad #1
Contact: [redacted] [redacted]

b2
b7E
b2
b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

b6
b7C

Case ID #: (U) 66F-HQ-C1364260 (Pending)
(U) 66F-HQ-C1384970 (Pending)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

b2
b7E

Synopsis: (U) The [redacted] is providing examples of utilization of USA Patriot Act provisions.

(SECRET) ~~Derived From : Multiple Sources~~
~~See Classification Authority Reference~~
~~Section.~~
~~Declassify On:~~ X1

Classification Authority Reference: ~~(S)~~ (U)

Details: (U) Reference FBIHQ (ILU,OGC) EC to All Field Offices dated 02/27/2004.

(U) The referenced EC requested that each field office provide statistics, examples or anecdotes, or a brief narrative summarizing the benefits which the office has received from the use of specified sunset provisions of the USA Patriot Act.

(U) Accordingly, the two appropriate [redacted] squads dealing with FCI/DT/IT and Cybercrime were contacted and the following information was provided:

b2
b7E

[redacted] (U)

b2
b7E

SECRET

To: General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/19/2004 b7D

(U) The FCI/DT/IT squad had one example each of its utilization of the Information Sharing provision and the Changes to the Primary Purpose Standard for FISA. The following are the examples provided, along with a comment regarding the New Standard for Business Records under FISA:

(U) I. Information Sharing

b1
b6
b7C

(S) [redacted] (S)

b1
b6
b7C

(S) [redacted] (S)

b1
b6
b7C

(S) [redacted] (S)

b1
b6
b7C

(S) [redacted] (S)

b1
b2
b7E
b7D

(S) [redacted] (S)

b1
b2
b7E

(S) [redacted] (S)

To: General Counsel From: [redacted]
Re: (U) 66F-HQ-C1364260, 03/19/2004

b2
b7E

[redacted] (S)

b1
b7D
b2
b7E

(U) II. Primary Purpose Clause

b1
b6
b7C

(S) [redacted] (S)

(S) [redacted] (S)

b1
b7D
b2
b7E

(S) [redacted] (S)

b1
b2
b7E

SECRET

To: General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/19/2004 b7E

b1

[redacted] (S)

(U) III. Commentary relating to the New Standard for Business Records under FISA

(U) [redacted]

[redacted] b5

◊◊

SECRET

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/19/2004

To: General Counsel ATTN: AGC [redacted] b6 b7C
Investigative Law Unit

From: [redacted] b2
Sqd 2
Contact: CDC [redacted] b7E b2

Approved By: [redacted] b6 b7C

Drafted By: [redacted] b6 b7C

Case ID #: 66F-HQ-C1364260-35 (Pending)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: To provide Investigative Law Unit with examples of usage of certain sunsetted provisions of the USA Patriot Act by the [redacted]

Details: Per the request contained in the OGC, ILU EC dated 2/27/2004, captioned as above, the following is a synopsis of instances where certain provisions of the USA Patriot Act, subject to being sunsetted on 12/31/2005, have been utilized by [redacted] b2 b7E

Nationwide Search Warrants for E-mail and Associated Records - Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

305C-[redacted]-42731 Nationwide search warrant for AOL. b2 b7E

On April 3, 2003, an FBI agent from [redacted], had signed onto America Online (AOL) in an undercover capacity. The agent had entered the AOL chat room [redacted] and encountered an individual using the AOL screen name [redacted] indicated that he was running a list management program in the chat room and advised that anyone wishing to join the list should type the words "list me." The Buffalo agent typed "list me" and shortly thereafter received an electronic mail (e-mail) message from [redacted] Embedded in the e-mail were nine images that depicted children engaged in sexual activity. The minors observed in these specific images had been previously identified through the FBI's Child Victim Identification Program. The agent subsequently initiated contact with [redacted] who then sent three additional e-mails to the agent. Two of the e-mails had an attached file that was a video clip of child pornography. The remaining e-mail again contained embedded images of child pornography. b6 b7C b2 b7E

Based on additional investigation [redacted] identified [redacted] as [redacted] a resident of [redacted] information was provided to [redacted] which continued the investigation of [redacted] A search warrant was eventually issued for [redacted] residence, at which time computer and other electronic evidence were seized. In an interview conducted during that search [redacted] admitted that he had engaged in the distribution and receipt of child pornography. Forensic examination of the electronic evidence supported the investigation; however, [redacted] sought to identify any additional evidence that [redacted] may have retained on AOL's server, in e-mail, etc. As such [redacted] has obtained a search warrant for [redacted] AOL account and intends to serve it during the week of March 15, 2004. It is anticipated that the warrant to be served upon AOL, located in Dulles, Virginia, will allow [redacted] to determine whether additional evidence regarding the distribution, receipt, or possession of child pornography resides in [redacted] account. In addition, [redacted] may be able to identify additional subjects, with whom [redacted] may have exchanged such images, or minors, with whom [redacted] may have been communicating.

b2
b7E
b6
b7C

[redacted] Nationwide search warrants issued as follows:
[redacted] to Hotmail and Verisign
[redacted] to Catalog.com, Yahoo!, Hotmail, and Verisign

b2
b7E
b7A

An international group of "carders" (individuals who use and trade stolen credit card information) was operating via the Internet using Internet Relay Chat channels and various fraudulently purchased web sites. The carders needed individuals within the United States to provide "drop" sites (addresses within the country of purchase to which fraudulently purchased goods could be delivered for shipment to locations outside of that country).

Nationwide search warrants were used to obtain e-mail communications among the carders. Search warrants issued on [redacted] provided information about the fraudulent activities of the group including a drop site in [redacted] In addition, e-mail addresses for other members of the group were discovered. Nationwide search warrants were then issued on [redacted] to obtain information from the newly discovered e-mail addresses as well as updating the information from the previously known addresses.

The content produced by the e-mail providers in response to the Nationwide search warrants resulted in the indictment of the individual operating the drop site located in [redacted] The Nationwide search warrants reduced the time needed to have the searches executed and significantly reduced the number of FBI, U.S. Attorney's Office, and Judicial personnel required to complete the search warrant process.

b7A

Intercepting Communications of Computer Trespassers - Section 217 of the Act clarified an ambiguity in the law by explicitly providing victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the communications sent or received by trespassers. Thus, this

section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting authorized users. Additionally, based on the definition of a "computer trespasser," communications of users who have a contractual relationship with the computer owner may not be monitored, even if their use is in violation of their contract terms (i.e. spammers). See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

b2
b7E
b7A

[redacted] Communications of Computer Trespasser Intercepted

An international group of "carders" (individuals who use and trade stolen credit card information) was operating via the Internet using Internet Relay Chat channels and various fraudulently purchased web sites. The carders would use proxy servers and free e-mail accounts to conceal their identities on the Internet. Proxy servers change an Internet users origin IP address to that of the proxy server such that only the proxy server knows the true point of origin. Free e-mail accounts can be obtained without providing true identification such as names, addresses, credit card numbers, etc. One such proxy server was located [redacted] and the [redacted] As a result, [redacted]. With consent from the server's owners, all Internet traffic that passed through the proxy port was intercepted in accordance with the above Patriot Act provision.

Prior to interception, two e-mail accounts were known for the main subject. The interception led to the discovery of three additional e-mail accounts used by the main subject. The only connection between the e-mail accounts was that the subject logged onto all of the accounts around the same time on numerous occasions. One of the newly discovered e-mail accounts provided a real name and physical address information for an individual in Kuwait believed to be the main subject. The other accounts provided additional leads that would not have been possible without the interception of trespasser communications (e.g. one of the other accounts was commonly used by the main subject in additional frauds making it simpler to identify the fraud and connect them to the subject).

Any questions concerning these cases may be directed to SSA [redacted] Sqd. 10 (Cyber) at [redacted] or SA [redacted]

b2
b6
b7C

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364260 03/19/2004 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

For information and possible use by ILU in support of continuing usage of certain provisions of the USA Patriot Act beyond 12/31/2005.

◊◊

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/16/2004

To: Office of the General Counsel **Attn:** [redacted]
Investigative Law Unit
Room 7326

From: [redacted]
C6/JTTF
Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) 66F-HQ-C1364260 (Pending)
(U) 66F-HQ-C1384970 (Pending)

DATE: 09-12-2005
CLASSIFIED BY 65179 DMH/KJ
REASON: 1.4 (C)
DECLASSIFY ON: 09-12-2030

05-CV-0845

Title: (U) USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: (U) Narrative of the benefits the [redacted] JTTF has received from certain provisions of the Patriot Act.

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) 66F-HQ-C1364260 Serial 58

Details: (U) ~~(S)~~ Per the referenced communication, the [redacted] JTTF would cite two significant investigations to support the renewal of the provisions of the Patriot Act that are scheduled to sunset on December 31, 2005.

[redacted] (S)

078IV03.EC

prior to the submission of the request. The new standard under Section 214 of the Patriot Act of "relevant to an ongoing investigation to protect against terrorism" could be established with the available evidence and the FISA request was approved within a few months.

(U) (S) Based in part on the data obtained from the pen registers, the case agent was able to establish that the subjects were in contact with the subjects of other FBI terrorism investigations.

(U) (S) This new information, combined with other information, provided a basis for a FISA request to authorize the interception of communications on the subject's cellular telephone. This request is pending approval. This investigation has been transferred to the Miami Division because the subject moved to Florida.

[redacted] (S) b1 b7A b2 b7E

[redacted] (S) b1 b7A

(U) (S) Further, it is anticipated that these records will support additional allegations into individuals who have previously been in control of money deposited into that account and may support a FISA request to overhear communications by the individual currently in control of those funds.

(U) (S) The information sharing provisions of the Patriot Act are now so routine for task force members that it

To: Office of the General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/16/2004 b7E

is almost unthinkable that these crucial tools would no longer be available.

[redacted] (S)

b1
b7A
b2
b7E

(U) (S) As one [redacted] JTTF member stated, b1
"because of the Patriot Act, one investigator can now pick up b7E
the phone and have information from ICE, the Postal Service, or the State Department at his fingertips." "It has created one-stop shopping" that has enhanced the speed at which we can recognize patterns of activity and can focus more quickly on a subject. Another investigator explained that he no longer wastes time trying to convince companies to provide information. They now comply immediately with requests because the Patriot Act obligates them to respond. "Investigations are no longer thwarted because of the timeliness of the response to the request for information."

(U) If requested, this Division will provide additional examples of how the passage of the Patriot Act has increased the ability of [redacted] investigators to obtain useful information into individuals and groups associated with terrorism. b2 b7E

SECRET

To: Office of the General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/16/2004 b7E

LEAD(s):

Set Lead 1: (Info)

ALL RECEIVING OFFICES

(U) Read and clear

◆◆

SECRET

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/18/2004

To: General Counsel **Attn:** Investigative Law Unit [redacted] b6 b7C

From: [redacted] b2
Squad 1
Contact: Acting OIC [redacted] b7E b6 b7C

Approved By: [redacted] b6 b7C

Drafted By: [redacted] b7C

Case ID #: 66F-HQ-C1364260 (Pending) ; 38
[redacted] (Pending) ; 8266 b7A

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: [redacted] response to USA Patriot Act survey regarding use of the particular provisions scheduled to expire on December 31, 2005. b2 b7E

Reference: 66F-HQ-1364260 Serial 5

Details: After a review of whether any of [redacted] investigations have utilized the enhanced investigative tools which are scheduled to expire as provided by the Patriot Act ("Act") [redacted] b2 b7E b1

[redacted] (S)

[redacted] has used other investigative tools created by provisions of the Act and these tools have had a crucial impact on [redacted] investigations. The greatest positive impact is derived from the ease with which [redacted] can now issue National Security Letters ("NSLs") due to the reduced signature authority of NSLs and the relevance standard. Before passage of the Act, NSLs were less frequently used because of the lengthy process required for issuance of NSLs. OGC has access to the control file that would provide an accurate number of NSLs issued since the passage of the Act. To supplement that figure, [redacted] polled the majority of the agents who have used NSLs on the number of NSLs used and the importance that obtaining such information in a timely manner was to their investigations. Based on that effort, it appears b2 b7E

~~SECRET~~

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364260, 03/18/2004 b7E

that [redacted] has issued well in excess of 100 NSLs since the passage of the Act. More importantly, the information obtained from these NSLs has represented the full range of information available to include financial records, E-mail account information, telephone toll records, and consumer credit reports. Invariably, the agents replied that the information was crucial to their investigations to the extent that the ability to succeed in the investigation hinged upon the ability to obtain such information in a timely manner. b2 b7E

Many of the cases in which the NSLs have produced positive impact are classified matters; accordingly, specific anecdotal examples will not be provided in this response. The Counter Terrorism squad supervisor has advised, in general terms, that the matters have concerned potential threats wherein the quick access to information from NSLs played a critical role in accessing the credibility of the potential threats. The Foreign Counter Intelligence squad has likewise show a dramatic increase in its utilization of NSLs and expressed the value that NSLs have provided to its efforts.

Furthermore, [redacted] anticipates that the new ability to obtain temporarily assigned network addresses by subpoena will play a critical role in its newly established Cyber Squad in intrusion cases. Thus far, that information has been already obtained by other divisions involved in the same investigations.

[redacted] will continue to educate its agents on the tools created by the Act, including the provisions scheduled to expire. If the investigative tools derived from the provisions with relevant expiration dates are employed in [redacted] prior to December 31, 2005, [redacted] will amend this response. b2 b7E

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364260, 03/18/2004 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Read and clear.

◆◆

~~SECRET~~

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

05-cv-0845

Precedence: ROUTINE **Date:** 03/17/2004

To: General Counsel **Attn:** [redacted] b6
Investigative Law Unit b7C
Room 7326

From: [redacted] b2
Squad A-1
Contact: CDC [redacted] b7E b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

DATE: 09-12-2005
CLASSIFIED BY 65179 DMH/KJ
REASON: 1.4 (C)
DECLASSIFY ON: 09-12-2030

05-CV-0845

Case ID #: 66F-HQ-C1364260 (Pending) - 39
[redacted] (Pending) - 8275
66F-[redacted]-C117669 (Pending) - 973

b2 b7E b7A

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: To provide information summarizing [redacted] reliance on several authorities implemented by the USA Patriot Act (the Act) which are subject to sunset provisions. b2 b7E

Details: As requested in an electronic communication (EC) dated 2/27/2004 to All Field Offices from the Office of the General Counsel, offices were requested to provide the Investigative Law Unit (ILU) with information, examples and/or statistics demonstrating the benefits the division has received from certain provisions of the Patriot Act.

Writer conducted a poll of all supervisors within the division seeking information described above. Based upon responses b2 b7E the poll, [redacted] provides the following information:

1. Voice Mail - Section 209 of the Act permits law enforcement to obtain a search warrant or court order for voice mail messages maintained by a communications provider under 18 USC 2510 or 2703.

[redacted] (S) b1 b2

2. Nationwide Search Warrants for e-mail - Section 220 of the Act permits the issuance of search warrants with nationwide jurisdiction to an electronic communications service provider under 18 USC 2703. b7E

[redacted] (S) b1 b2 b7E

~~SECRET~~

3. Voluntary Disclosures by ISPs - Section 212 of the Act permits communications providers to voluntarily disclose the contents of communications to protect life or limb or their rights or property.

[redacted] b1 b2 (S) b7E

which involved a domestic terrorism investigation arising from an arson allegedly perpetrated by a radical animal rights group.

4. Information Sharing - Sections 203(b) and (d) of the Act permit the sharing of information between criminal and intelligence investigations. (S)

b1 [redacted]

b2 There is an overwhelmingly positive response among both criminal and intelligence investigators to this section of the Act. The examples b7E of information sharing are too numerous to describe in detail, however, two large scale investigations have benefitted immeasurably, specifically:

a. Example A is a criminal case which involves two charitable organizations found to have fund-raising ties to terrorist groups. The matter began as an intelligence investigation, but information was shared between criminal and intelligence investigators and will likely lead to criminal indictments and substantial forfeiture.

b. Example B is a criminal investigation into a Middle East terrorist group, with a parallel intelligence investigation into specific members of the group. Through information sharing and the ability of the criminal and intelligence investigators to work together, FISA interceptions and search warrants have been used to provide extremely valuable information for both the criminal and intelligence investigators.

5. Intercepting Communications of Computer Trespassers - Section 217 of the Act permits a computer owner/operator to provide consent for law enforcement to monitor the activities of a computer trespasser.

[redacted] (S) b1 b2

6. Expanded Title III Predicates - Sections 201 and 202 of the Act permit the use of court authorized electronic surveillance in b7E investigations involving chemical weapons, terrorism or computer fraud and abuse.

[redacted] (S) b1 b2 b7E

7. Roving FISA Surveillance - Section 206 of the Act permits roving surveillance where the target is attempting to thwart electronic surveillance.

[redacted] (S) [redacted] did assist another field office in its utilization of a roving FISA. Agents from the [redacted] Division monitored the roving FISA when the subject arrived in [redacted] and while the subject stayed in an area hotel. b1 b2 b7D b7E

8. New Standard for FISA Pen/Trap - Section 214 of the Act authorized a FISA order for a pen register or trap and trace device, based upon the standard that such is relevant to the investigation. b1 b2

[redacted] (S) b7E

9. Changes to the "Primary Purpose" standard for FISA Court Orders - Section 218 of the Act authorized the issuance of a FISA Court order where foreign intelligence gathering is a "significant purpose" rather than the "primary purpose."

[redacted] as sharing of information between intelligence and criminal agents was prohibited prior to the Patriot Act. See Examples 4a and b above. (S) b1 b2 b7E

10. New Standard for Business Records Under FISA - Section 215 of the Act permits the issuance of a FISA Court Order for records production where the information is relevant to an investigation.

[redacted] (S) b1 b2 b7E

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364260 03/17/2004 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

To provide information as requested by ILU. Read and clear.

◊◊

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/23/2004

b6
b7C

To: Office of the General Counsel **Attn:** [redacted]
Investigative Law Unit
Room 7326

From: [redacted]
L-1
Contact: ADC [redacted]

b2
b7E

Approved By: [redacted]

b6
b7C

Drafted By: [redacted]

Case ID #: 66F-HQ-C1364260 (Pending)
[redacted] (Pending)

b2
b7E

Title: USA PATRIOT ACT
SUNSET PROVISIONS

b7A

Synopsis: To provide the Investigative Law Unit, Office of the General Counsel (OGC) the information requested via their EC dated 1/23/04 regarding captioned matter.

Details: Pursuant to the above referenced request a canvass of all [redacted] squads was conducted to obtain statistics, good example and/or narratives summarizing the benefits [redacted] has received from the referenced sunset provisions. The result are as follows:

b2
b7E

Information Sharing- Section 203(b): This section of the sunset provision was of great benefit to criminal and intelligence matters being investigated. Having a hard wall again between intelligence and criminal matters would greatly inhibit law enforcement ability to conduct long term terrorism investigations, which often falls into both categories.

[redacted] with hotmail.com (S) in regards to 315N matter. This act was also used in the same case to obtain information from yahoo.com, with unsuccessful results.

b1

New Standard for FISA Pen/Trap- Section 214: [redacted] in two [redacted] 315N matter. (S)

b1
b2
b7E

66F-HQ-C1364260-40

To: Office of the General Counsel From: Miami
Re: 66F-HQ-C136426 03/23/2004

Change to Primary Purpose Standard for FISA Section 218: [redacted] b1 (S)

To date, the other sunset provisions of the Patriot Act have not been used in the [redacted] lead is considered covered. b2 b7E

◊◊

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 03/19/2004 **Date:** 03/19/2004

To: General Counsel **Attn:** [redacted] Room 7326 b6

From: [redacted] b2 b7C
Office of Division Counsel (ODC) b7E

Approved By: [redacted]

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-09-2005 BY 65179 DMH/KJ

Case ID #: 66F-HQ-C1364260 (Pending) b2
66F-[redacted]C1384970 (Pending) 05-CV-0845 b6 7E
66-[redacted]-5618 b7C

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: To advise the Office of the General Counsel (OGC) of provisions of the Patriot Act used by [redacted] that are set to expire on 12/31/2005. b2 b7E

Reference: 66F-HQ-C1364260 Serial 5
66F-HQ-C1384970 Serial 7564

Details: Referenced Bureau communication requested field offices to report the usage of provisions of the USA Patriot Act set to expire on 12/31/2005. [redacted] has used several of these provisions to its investigative advantage in general criminal and counterintelligence cases, but has made the most use of these provisions in counterterrorism cases. Initially, however, [redacted] reports that Agents on several occasions have requested to make appropriate use of important tools legislated in the Patriot Act and each request has been denied by the Department of Justice (DOJ), Office of Intelligence Policy and Review (OIPR). Specifically, [redacted] has requested OIPR approval for "roving FISA surveillance" under Section 206 regarding known Intelligence Officers (IOs) who employ counterintelligence techniques to avoid detection. All of [redacted] requests have been denied. In addition, WFO has requested the use of the new standard to obtain business records under FISA and has been denied on each occasion. [redacted] notes that the same records may be obtained in criminal cases by b2 b7E

use of subpoena, yet the legislated tool in counterintelligence and counterterrorism cases goes unused.[1]

In regard to Section 220 and the ability to obtain nation-wide search warrants, [redacted] has benefitted not only in regard to the efficiency in which it can conduct its own investigations [redacted], but also in regard to the personnel resources it does not have to expend in obtaining search warrants to be served in America On Line (AOL). In the past [redacted] had expended significant resources in regard to the liaison with the U.S. Attorney's Office in the Eastern District of Virginia in drafting, and applying for AOL search warrants, as well as the service of these warrants. b2 b7E b7A

[redacted] has used the authority in Section 212 of the Patriot Act on occasions when the Assistant Director or the Special Agent in Charge has found that information developed revealed an emergency involving an immediate risk of death or serious injury. In a number of cases, this provision allowed [redacted] to obtain the content of e-mail in response to threats (usually over the Internet or e-mail), where the use of other more routine provisions would have been much less timely or would have required specific approval by the Attorney General. [redacted] used this provision to obtain access to e-mails wherein members of a known terrorist group had e-mail traffic involving a discussed attack (315S-[redacted]-224164). The provision was also used in investigating a threat to a high ranking foreign official. b2 b7E

The new information sharing procedures of Section 203(b) & (d) and the changes to the "primary purpose" standard for FISA have significantly changed the way [redacted] investigates terrorism cases for both intelligence value and for criminal prosecution. [redacted] has participated in numerous investigations in the last two years that have involved the participation of investigators in foreign countries, criminal investigative techniques, Assistant United States Attorneys and the use of FISA. On several occasions, [redacted] has obtained the express authorization of the Attorney General to use FISA information in criminal proceedings. Case Agents and others have commented that these investigations would never have operated as smoothly prior to these Patriot Act provisions, and in some cases, the matters would have been almost impossible to complete. These changes were most evident in [redacted] 315O-[redacted]215590,and in the b2 b7E b7A

[1] [redacted] b2 b7E

"Virginia Jihad" series of cases. In addition, the "significant purpose" standard has allowed the employment of the FISA technique on indicted individuals, wherein significant foreign intelligence has been developed. Such use of this technique would not have been practically employed in the past under DOJ's reading of the "primary purpose" standard.

Section 214 of the Patriot Act has enabled Agents conducting CI/CT investigations to obtain pen register data on the subjects of their investigations in a way that is much more like the way their counterparts on the criminal side obtain such authorization. However, significant resources could still be saved by streamlining the process even further, by giving FBI attorneys access to the FISA judges and by creating positions for FISA magistrates. Pen register/trap trace is an important investigative tool and could be used to a greater extent if the process is made easier. It has provided useful and invaluable information (65A[redacted]220066) regarding previously unknown contacts on case subjects that may have gone unknown before when there was a requirement to identify the individual as an agent of a foreign power. b2 b7E

[redacted] believes that all of these provisions, if utilized to their fullest intended extent, are useful tools and should be extended. Further, OGC and Congressional Affairs should continue to seek further legislation to assist in investigative efforts.

LEAD(s):

Set Lead 1: (Discretionary)

GENERAL COUNSEL

AT WASHINGTON, DC

Will include [redacted]use of the Patriot Act in justification to remove expiration dates from the various described provisions. b2 b7E

♦♦

SECRET

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/24/2004

To: General Counsel **Attn:** Investigative Law Unit, FBIHQ
Room 7326, [redacted] b6 b7C

From: [redacted] b2
Chief Division Counsel b7E
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE b2 b6 b7C

DATE: 09-12-2005 b6
CLASSIFIED BY 65179 DMH/KJ
REASON: 1.4 (C) b7C
DECLASSIFY ON: 09-12-2030

Case ID #: 66F-HQ-C1364260-44 (Pending)
1A[redacted]231 b2
05-CV-0845 b7E

Title: USA PATRIOT ACT SUNSET PROVISIONS

Synopsis: [redacted] summary of the benefits the office has received from Patriot Act provisions which will sunset or expire on December 31, 2005, unless Congress acts otherwise. b2 b7E

Details: The [redacted] has canvassed individuals who have used some of the Patriot Act investigative tools outlined in serial 5, dated February 27, 2004, in file 66F-HQ-C1364260. The following summary includes only those tools used or actively considered by the Division.

Roving FISA Surveillance-Section 206

[redacted] (S) b1 b2

The Case Agent, [redacted] characterized this authority as both necessary and effective. While the roving authority did not thwart a terrorist act, it better enabled the Agents to successfully and more expeditiously conclude the investigation. All participants agreed that the option to consider securing this authority is critical in resolving serious IT and FCI matters. b7E b6 b7C

New Standard for FISA Pen/Trap

For reasons of which OGC is aware, the lower evidentiary standard to establish grounds to secure FISA pen/traps has not been adequately exploited in IT and FCI

SECRET

b2
b7E

matters. [redacted] has submitted some requests, but until the process is expedited and made more akin to the ease with which criminal pen/traps are secured, the law has been of little benefit. In fact, in at least one 315 case, criminal pen/trap orders (and grand subpoenas) were used largely because of the perceived slow pace in using FISA techniques, despite the fact that a full content FISA was later approved. [redacted] (S)

b1
b2
b7E

Changes to "Primary Purpose" Standard for FISA

The change to the FISA certification now requiring that foreign intelligence be a "significant purpose" of the authority sought has benefitted the FBI's mission in general, and [redacted] investigations in particular, as it has made considering and/or obtaining FISAs more possible under appropriate circumstances. If nothing else, it has also given Agents more flexibility in determining how to most effectively use investigative strategies to protect against terrorism and clandestine intelligence activities. And similarly, consultation with prosecutors has improved.

b2
b7E

New Standard for Business Records for FISA

b1
b2
b7E

[redacted] notes the process would appear to be greatly improved based on recent changes allowing FBIHQ/OGC to bypass OIPR, but the benefits have not been fully realized yet. (S)

♦♦

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C136426 03/24/2004 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

For information and possible use by ILU in support of continuing usage of certain provisions of the USA Patriot Act beyond 12/31/2005.

♦♦

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

b7

Precedence: PRIORITY **Date:** 03/22/2004

To: General Counsel **Attn:** Investigative Law Unit
[redacted]
Room 7326

b6
b7C

From: [redacted]
Legal Unit
Contact: ADC [redacted]

b2
b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

b2
b6
b7C

Case ID #: 66F-HQ-C1364260 (Pending) - 46
[redacted] (Pending) - 8390
197-[redacted]-C233355 (Pending) - 4

b7A
b2

Title: USA PATRIOT ACT
SUNSET PROVISIONS

b7E

Synopsis: To provide [redacted] response to request for examples and summaries of use of investigative tools created by the USA PATRIOT Act. Lead covered.

b2
b7E

Reference: 66F-HQ-C134260 Serial 5

Details: This EC provides a brief narrative summarizing [redacted] use of investigative tools created by the USA PATRIOT Act. A canvas was conducted of all squads in the Los Angeles Division and the following details the results:

Voice Mail - Section 209 of the Act enabled law enforcement to obtain all voice mail which is stored by a communications provider, including unopened voice mail, using the procedures set forth in 18 U.S.C. §2703 (such as a search warrant). This also applies to other wire communications as defined by the statute. Voice messages stored and in the possession of the user, such as messages on an answering machine, are not covered by this statute. Previously the law was vague on the standard required to compel production of a stored voice mail message, leaving the possibility for argument that a wiretap order was required. See 18 U.S.C. § 2510; 18 U.S.C. § 2703.

[redacted] (S)

b1
b2
b7E

~~SECRET~~

To: General Counsel Fr[redacted]: [redacted] b2
Re: 66F-HQ-C1364260, 03/22/2004 b7E

Nationwide Search Warrants for E-mail and Associated Records - Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

This technique was utilized by the [redacted] following the shooting on July 4, 2002 at [redacted] International Airport. It was extremely helpful in this investigation for the Central District of California to be able to issue nationwide search warrants for information on the subject's email. b2 b7E

Voluntary Disclosures - Section 212 of the law explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers. This provision also allows a communications service provider to disclose non-content records to protect their rights and property. This portion of the provision will most often be used when the communications service provider itself is a victim of computer hacking. See 18 U.S.C. § 2702(b) & (c)(3); 18 U.S.C. § 2703(c)(2)(F).

For about ten months (January 2003-November 2003) there was a mandatory reporting requirement for the receipt of content information (usually e-mail content) under this emergency disclosure provision. (See the Homeland Security Act and EC 66F-HQ-C1384970 Serial 501.) During that time, offices were only required to report the number of e-mail messages that were received under this voluntary disclosure provision. Offices were not required to report the receipt of records and were also not required to provide case information. For this reason, it would be beneficial for offices to now report more detail on these voluntary disclosures. Examples where voluntary disclosures led to valuable foreign intelligence or arrests would be particularly helpful.

[redacted] (S) b1
Moreover, this was the practice after 9-11, where service providers voluntarily provided FBI Los Angeles with the information requested. In an emergency or crisis situation it would be imperative to the investigation for b2 b7E

service providers to have this ability to voluntarily provide the FBI with this information. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly. This is what occurred after 9-11 and should continue to be in place in the eventuality of another such attack.

Information Sharing - Section 203(b) & (d) of the Act provided new information sharing capabilities between criminal and intelligence investigations for foreign intelligence information and information obtained via a Title III electronic surveillance. (See EC [redacted] dated 10/26/01 for additional information.) Recognizing that this tool has become a regular part of how the FBI operates, especially in terrorism cases, no statistics are necessary. However, case examples that demonstrate the importance of this tool should be provided. b7A

All [redacted] CT and CI investigation continue to benefit from this provision of the USA PATRIOT Act. A good example of this in Los Angeles is the case where the intelligence investigation of an FBI Supervisory Special Agent and a member of the PRC revealed information that the intelligence squad was able to share with a criminal squad for prosecution on criminal charges. Information sharing has also been invaluable between CT/CI investigations and criminal investigations into violations of neutrality, fraudulent document production, passport/visa violations, immigration violations, white collar crimes, drug cases, and all types of fraud schemes. b2 b7E

Intercepting Communications of Computer Trespassers - Section 217 of the Act clarified an ambiguity in the law by explicitly providing victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting authorized users. Additionally, based on the definition of a "computer

trespasser," communications of users who have a contractual relationship with the computer owner may not be monitored, even if their use is in violation of their contract terms (i.e. spammers). See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

This provision has proven especially useful to the [redacted] and is considered a key aspect of all cyber investigations. "Hackers" routinely use victim computers for SPAM and other illegal communications. Therefore, this provision has proven useful in both intelligence and criminal investigations. Recently this method has been used on at least two occasions in intelligence cases where the FBI took over the victim's on-line identity to communicate with the suspected terrorists. b2 b7E

Expanded Predicates for Title III - Sections 201 & 202 of the Act expanded the predicate offenses for Title III to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). See 18 U.S.C. § 2516. b1 b2 b7E

[redacted] (S)

yet but it is anticipated that the expanded predicate offenses for computer fraud and abuse will become essential to several Los Angeles investigations.

Roving FISA Surveillance - Section 206 amended FISA to allow the Court to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in trade craft designed to defeat electronic surveillance, such as by rapidly switching cell phones, Internet accounts, or meeting venues, the Court can issue an order directing "other persons," i.e., the as yet unknown cell phone carrier, Internet service provider, etc., to effect the authorized electronic surveillance. Even if the target is not engaged in obvious trade craft, we can obtain such an order as long as the target's actions may have the effect of thwarting surveillance. This allows the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. For additional information see EC [redacted] dated 10/26/01. Any examples where roving authority has been obtained and utilized to gain valuable foreign intelligence should be provided. b7A

The roving wiretap provision has been extremely helpful in [redacted] One specific example is that Los Angeles has b2 b7E

seen counterintelligence targets change service for hard-lines, email accounts, and cell phones numerous times. The roving FISA authority has allowed for investigators to continuously monitor these targets without interruption. Changing of telephone carriers is a documented technique used by foreign intelligence officers to avoid detection. [redacted] has documented these occurrences and been able to continue coverage because of this provision. b2 b7E

New Standard for FISA Pen/Trap - Section 214 of the Act eliminated the requirement that the FISA pen/trap order include specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." For additional information see EC [redacted] dated 10/26/01. b7A

This provision has not proven useful to [redacted] Although the standard has been lowered the reality of the work load situation at OIPR makes this technique not viable. With the creation of the 315 classification, an agent has much better luck with getting a pen register under criminal standards than waiting for a FISA pen register to be approved. Moreover, if agents are going to take the time to fill out the paperwork for the FISA pen register, they might as well complete an actual FISA application. In one example, an agent was told she had enough for a FISA and not to waste time with the pen register. In another situation, the agent made the pen register request first and then several months later requested the FISA and never again heard anything on the pen register. If this was something that could be approved at HQ or locally, then it might be a valuable technique, but with the backlog on FISAs it is impractical to request a pen register FISA and then wait months to hear nothing. b2 b7E

Changes to "Primary Purpose" Standard for FISA - Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such

consultation does not, in itself, undermine the required certification of "significant purpose." These changes allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk. For additional information see EC 66F-HQ-A1247863 Serial 71 dated 10/26/01. While no statistics are required for this provision, case examples and brief narratives on the benefits of this provision are sought.

This is the single most important provision of the USA Patriot Act. [redacted] investigations have revealed that more often than not the suspected terrorists or intelligence officers are committing criminal violations in support of their terrorist activities. The ability to obtain a FISA order where there is substantial evidence of criminal activity and significant evidence that the proceeds are then being used to fund terrorist activities is imperative to these types of investigations. This provision also goes hand-in-hand with the information sharing provision. The shift in focus allows investigators to coordinate more with AUSAs and other law enforcement information regarding the criminal activities of terrorists. b2 b7E

New Standard for Business Records under FISA - Section 215 changed the business records authority found in Title V of FISA. The old language allowed the FISA Court to issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. Section 215 changed this standard to simple relevance (just as in the FISA pen register standard described above) and gave the Court the authority to compel production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This is the same standard described above for Section 214. For additional information see EC [redacted] 71 dated 10/26/01. b7A

Although [redacted] views this as an extremely valuable technique [redacted] (S)

[redacted] is aware of efforts by NSLB to resolve this issue with OIPR. [redacted] would argue that this is an extremely valuable technique because of the ability to obtain records where an NSL is not appropriate. The standard of simple relevancy should be sufficient for these b1 b2 b7E

To: General Counsel From: [redacted]
Re: 66F-HQ-C1364260, 03/22/2004

b2
b7E

investigations. NSLB should make all attempts to enforce this standard and not permit OIPR to create a higher standard which would make use of this technique more difficult.

[redacted] considers this lead covered.

To: General Counsel From: [redacted]
Re: 66F-HQ-C1364260, 03/22/2004

b2
b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Investigative Law Unit: Read and clear.

◆◆

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

Precedence: PRIORITY **Date:** 03/19/2004

To: General Counsel **Attn:** Investigative Law Unit, AGC [redacted]

From: [redacted] b2
Squad 2
Contact: CDC [redacted] b7E [redacted] b2 b6 b7C

Approved By: [redacted] b6 b7C

Drafted By: [redacted] DMK

46

Case ID #: (U) 66F-HQ-C1364260 (Pending)
(U) 66F-HQ-C1384970 - 8401

Title: (U) USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: (U) To provide Investigative Law Unit (ILU), Office of the General Counsel (OGC), with statistics and examples of the benefits [redacted] has derived from specified provisions of the USA PATRIOT Act. b2 b7E

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) 66F-HQ-C1364260 Serial 5

Details: (U) Referenced communication instructed all field offices to provide ILU with statistics, examples and/or a brief narrative summarizing the benefits each division has derived from specified provisions of the USA PATRIOT Act.

(S) Referenced communication set forth a list of specific techniques for which each field office is to report statistics concerning its use. [redacted] (S)

~~SECRET~~

b1
b2
b7E

1-D

~~SECRET~~

SECRET

b2

To: General Counsel From: [redacted] b7E
Re: (U) 66F-HQ-C1364260, 03/19/2004

[redacted] (S)

b1
b2
b7E

(U) Set forth below are statistics and/or descriptions concerning Milwaukee Division's use of the remaining specified techniques:

[redacted] (S)

b1
b2
b7E

(U) (S) The [redacted] would clearly have submitted additional requests for such orders in a number of other cases but for the fact that, to date, no such orders have ever been issued. [redacted] experience is that FISA business record orders are likely to prove essential in numerous investigations once they begin to be issued.

b2
b7E

[redacted] (S)

b1
b2
b7E

(U) (S) One of the two exceptions noted above pertained to an individual who ultimately became the target of a FISA full content interception. [redacted] therefore believes that pen and trap order could still have been obtained in that instance under the previous, higher, standard. With regard to the second exception, although a foreign power was identified, [redacted] believes it would still have been difficult to meet the prior standard. Furthermore, the time involved with obtaining the

b2
b7E

b2
b7E

facts necessary to support the affidavit would have probably resulted in missing the window of opportunity for deploying the technique. b2 b7E

(S) 315N (S)

classification investigations (none of which are in conjunction with an application for an order authorizing the interception of the content of communications). While each instance meets the current "relevancy" standard, it is questionable whether any of these three orders could be obtained under the previous, higher, standard. b1 b2 b7E

(U) (S) Changes to the Primary Purpose Standard: This change, which removed the risk of having to shut down the Division's most productive FISC authorized techniques in the event information was shared with prosecutive personnel, has directly let to a dramatic improvement in case coordination (see "information sharing" below). The change in the Primary Purpose standard, and consequent removal of "the wall," has fundamentally changed and enhanced the manner in which the conducts international terrorism and foreign counterintelligence investigations.

(U) (S) Information Sharing: Due to elimination of the Primary Purpose standard, sharing of information with regard to terrorism investigations has become routine. It is now standard practice that all 315 classification cases are reviewed for federal criminal prosecutive potential by appropriately cleared United States Attorney's Office personnel. The changes in this area have led to US Attorney personnel being incorporated as essential and integral components of JTTFs in both headquarters city and the Madison Resident Agency. b2 b7E

(U) (S) For example, the First Assistance United States Attorney, has FBI office access, a desk in JTTF office space and a GroupWise account. He is continually (almost daily) briefed on significant cases. In fact, the US Attorney's Office Intelligence Officer assigned to FBI JTTF actually serves as the Coordinator of that JTTF. b2 b7E

(U) (S) Similar coordination occurs with regard to the United States Attorney's Office, and the JTTF located in the Resident Agency. b2 b7E

SECRET

To: General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/19/2004 b7E

[redacted] (S)

b1
b2
b7E
b6
b7C
b7A

investigation.

(U) While information sharing is a rather novel concept with regard to FCI investigations, its importance to [redacted] efforts in this area also cannot be overstated. Traditionally, FCI investigations have been hamstrung by rules that did not allow investigators to consult with prosecutors until the investigation was essentially over. Specific examples of the benefits which the new rules have brought to FCI investigations in [redacted] include the United States Attorney's Office [redacted] providing advice and consent to seize and initiate forfeiture of $30,000 which was brought into the United States illegally by the subject of a 200M investigation. The US Attorney's Office has also provided counsel in [redacted] FCI cases regarding violations of the Foreign Agent Registration Act. b2 b7E

SECRET

To: General Counsel From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 03/19/2004 b7E

LEAD(s):

Set Lead 1: (Information Only)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) This information is provided for appropriate use by the Investigative Law Unit.

♦♦

SECRET

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 03/31/2004

To: OGC **Attn:** ILU, room 7326

From: [redacted]
Legal
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: ~~66F~~-HQ-C1364260 (PENDING)
66F-HQ-C1384970

Title: USA Patriot Act
Sunset Provisions

DATE: 09-12-2005
CLASSIFIED BY 65179 DMH/KJ
REASON: 1.4 (C)
DECLASSIFY ON: 09-12-2030

05-CV-0845

Synopsis: Use of Sunset Provisions of USA Patriot Act by [redacted]

Reference: [redacted]

Details: Between 03/25/04 and 03/30/04, writer contacted the four counter terrorism supervisors, two counter intelligence supervisors, and four SSRAs in the [redacted] as to the uses of the Sunset Provisions of the USA Patriot Act. Many of the supervisors stated that their numbers were approximate and other instances of the use of these provisions were possible prior the supervisor assuming leadership of the squad. All of the supervisors agreed that the Sunset Provisions are very useful and necessary in the war on terrorism.

The following are the number of instances that the Houston Division has reported utilizing each of the Sunset Provisions:

Section 209 [redacted] (S)
Section 220
Section 212
Section 203

b6
b7C
b2
b7E
b2 , b6, b7C
b6
b7C
b2
b7E
b7A
b2
b7E
b1
b2
b7E

~~SECRET~~

093 cd 005

b2

To: OGC From: [redacted] b7E
Re: 66F-HQ-C136426 (PENDING), 03/31/2004

Section 217
Section 201
Section 206
Section 214
Section 218
Section 215

[redacted] (S)

b1
b2
b7E

* Virtually all of the supervisors spoke to the necessity of the Section 203 (b) and (c), the Information Sharing provision. It universally was lauded as a major step forward in the war on terrorism. [redacted] utilized contacts with [redacted] in the development of the case. One counter intelligence supervisor cited 4-5 cases where the FBI could not have made a case on terrorism, but for contacts with the United States Intelligence community. Information sharing was utilized heavily in putting together terrorism watch plans for the 2004 Super Bowl and 2004 Baseball-All Star Game. Three other supervisors cited sensitive cases made, or greatly assisted by, our newly obtained ability to share information with the intelligence community.

b2
b7E
b7A

** One squad was in the process of attempting to utilize section 201 and 202 (Expanded Title III predicates), but, because of an emergency, utilized a FISA instead of a Title III.

*** One supervisor stated that even though his squad did not utilize the traditional roving FISA Surveillance as explained in Section 206, he had FISA search warrants authority granted for all vehicles being utilized by his squad's targets.
♦♦

(Rev. 01-31-2003)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 08-24-2005
CLASSIFIED BY 65179 DMH/KJ
REASON: 1.4 (c)
DECLASSIFY ON: 08-24-2030

FEDERAL BUREAU OF INVESTIGATION

05-cv-0845

Precedence: ROUTINE **Date:** 03/19/2004

To: General Counsel **Attn:** [redacted]
Investigative Law Unit
FBIHQ Room 7326

From: [redacted]
Squad #2
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 66F-HQ-C1364260 (Pending)
66F-HQ-C1384970 (Pending)

Title: USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: To respond to the Office of General Counsel (OGC) regarding captioned matter.

Details: For information of OGC, by EC dated 02/27/2004, OGC requested field divisions provide examples, statistics, anecdotal information and brief narratives summarizing the benefits derived by the office through the use of these provisions.

The following provisions have been used by the [redacted]

Nationwide Search Warrants for E-mail and Associated records:

This provision has been used several times in Child Exploitation Matters (305 cases).

In one instance, a subject in [redacted] downloaded illegal child pornography images from a server located in Fremont, California. A search warrant utilizing this provision was obtained in the [redacted] for records in the server located in Fremont, California.

In another 305 matter, Nationwide Search warrants were used to obtain evidence from AOL, Yahoo, and 23 photo albums located on a server in the [redacted]

This provision was utilized in [redacted] additional 305 investigations. (S)

b6
b7C
b2
b7E
b1

SCANNED COPY FILED IN
66F-HQ-1384970-8611

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364260, 03/19/2004 b7E

b1
b2
b7E

New Standard for FISA Pen/Trap:

[redacted] The new standard of "relevant to an ongoing investigation" was critical in obtaining a pen/trap and the information obtained through the pen/trap will lead to a full investigation. (S)

Information Sharing: Section 203 (b) & (d)

This provision has been the most helpful and has been used the most throughout the division. Specifically the case where the most impact was observed is the investigation of the Palestinian Islamic Jihad (PIJ) and [redacted] Specifically, before "the wall" came down, the presence of "the wall" had a negative impact on the ability of the criminal investigators to develop a viable criminal case for prosecution. There was approximately nine (9) years of FISA take that couldn't be shared with the criminal investigators. The majority of the PIJ indictment was prepared in Mid-2002, prior to "the wall" coming down, utilizing information that had been formally passed over "the wall" with appropriate authority and after substantial effort by both criminal and intelligence investigators. This information consisted of approximately 250 FISA-derived conversations and approximately 100 FISA-derived faxes. b6 b7C

After "the wall" came down, in approximately January 2003, over 20,000 hours of FISA-derived intercepts became immediately available for use by the criminal investigators, which included thousands of calls previously deemed to be pertinent. Although welcome, it created a significant information overload. Consequently the criminal investigation is still ongoing, but clearly, bringing down "the wall" allowed criminal investigators the opportunity to enhance their investigation, which was already set for indictment, in spite of "the wall." The criminal investigators and prosecutors now have a clearer understanding of the criminal activities of the PIJ, because all pertinent information in possession of the FBI is now available for their use.

In addition to information sharing "in-house," this provision has broadened the sharing between federal and state and local agencies. This broadened sharing between agencies has encouraged a regular interaction between investigators. In a specific case in Orlando, information sharing has led to joint investigations or subjects in the group. Through coordination and sharing, Tampa has been able to place leaders of the targeted group in [redacted] which prevented them from returning to the U.S. after departing. (S)

b1

~~SECRET~~

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364200, 03/19/2004 b7E

b1
b2
b7E

[redacted] (S)

~~SECRET~~

To: General Counsel From: [redacted] b2
Re: 66F-HQ-C1364210, 03/19/2004 b7E

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

Read and Clear

♦♦

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 17
Page 1 ~ Referral/Direct
Page 2 ~ Referral/Direct
Page 3 ~ Referral/Direct
Page 4 ~ Referral/Direct
Page 5 ~ Referral/Direct
Page 6 ~ Referral/Direct
Page 7 ~ Referral/Direct
Page 8 ~ Referral/Direct
Page 9 ~ Referral/Direct
Page 10 ~ Referral/Direct
Page 11 ~ Referral/Direct
Page 12 ~ Referral/Direct
Page 13 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 16 ~ Duplicate
Page 17 ~ Duplicate

Attn: [redacted]

b6 , b7C

Subject: Attn: [redacted]
Date: Fri, 6 Sep 20[redacted] 10:21:58 -0400
From: "[redacted]" <[redacted]>
To: <nationalpress@FBI.GOV>

b6
b7C

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-15-2005 BY 65179 dmh/ljm ca#05-cv-0845

Hi, [redacted]

Thank you for your assistance.
Following are the questions I would like to ask of a spokesperson for the FBI with regard to the events of Sept. 11, 2001, and the passage of the Patriot Act in October 2001. But first, I would like to explain how I plan to use these comments.
Our staff is preparing an article that will reflect upon the events of Sept. 11, 2001, and the passage of the Patriot Act, and how those events have changed the financial crimes arena, particularly with regard to money laundering. As a sidebar to the main article, we are asking several key figures on the money laundering front to share their general thoughts and comments on the past year's events and how they have changed the operation of their agencies and organizations. The article will be very straightforward and simple, featuring just one or two direct quotes from each of our contacts.

Here are the questions:

1. What did 9-11 and the passage of the Patriot Act mean to your agency?

2. Could you share some specific details as to how things have changed within your agency?

3. Have you had to enhance the training of your staff? If so, to what extent and how did you carry out that training?

4. Has the level of communication changed between your agency and other government agencies that deal with money laundering? If so, how has it changed?

Thank you for offering to pass these questions along to someone -- either [redacted] or another spokesperson. I appreciate your assistance.

b6
b7C

Regards,

[redacted]

b6
b7C

Tel. [redacted] ext. [redacted]
Fax [redacted]

[redacted]

b6
b7C

9/10/02 Declined. YM

ORIGINAL

80-HQ-1199962-2693

9/6/2002 10:30 AM

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 4
Page 1 ~ Referral/Direct
Page 2 ~ Referral/Direct
Page 3 ~ Referral/Direct
Page 4 ~ Referral/Direct

SUNSET PROVISIONS IN BOLD

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.

Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.

Sec. 203. Authority to share criminal investigative information.
203 (b) (Title III) and (d) (Grand Jury)

Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.

Sec. 205. Employment of translators by the Federal Bureau of Investigation.

Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.

Sec. 208. Designation of judges.

Sec. 209. Seizure of voice-mail messages pursuant to warrants.

Sec. 210. Scope of subpoenas for records of electronic communications.

Sec. 211. Clarification of scope.

Sec. 212. Emergency disclosure of electronic communications to protect life and limb.

Sec. 213. Authority for delaying notice of the execution of a warrant.

Sec. 214. Pen register and trap and trace authority under FISA.

Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act.

Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices.

Sec. 217. Interception of computer trespasser communications.

Sec. 218. Foreign intelligence information.

Sec. 219. Single-jurisdiction search warrants for terrorism.

What did Patriot Act do?

1. Enlarged ELSUR capabilities
   - 201 and 202 added predicate terrorism-related offenses for T-III
   - 206 - Roving wiretap
   - 207 - extended duration of FISA
   - 209 - voice mail with a search warrant
   - 214 - FISA Pen standard made congruent with criminal standard
   - 216 - nationwide effect of pen/trap orders
   - 217 - computer trespasser
   - 218 - FISA "purpose" changed to 'significant purpose"
   - 220 - nationwide search warrants for e-mail
   - 225 - civil liability immunity for compliance with FISA order

2. Encouraged sharing of information
   - 203 (a) - Grand Jury information
   - 203(b) - Title III information
   - 203(d) - Any foreign intelligence information
   - 901 & 905 - coordination between DCI and FBI

3. Made intelligence investigative techniques congruent with criminal techniques
   - 206 - Roving wiretap authority
   - 214 - Pen/trap standard
   - 215 - Standard for business records
   - 505 - Standard for NSLs

4. Expanded anti-terrorism financial tools
   - 314 - enhance USG/financial institution cooperation re: money laundering
   - 315 - expand money laundering predicates
   - 317 & 318 - long-arm jurisdiction over foreign money-launderers
   - 319 - jurisdiction over foreign funds in U.S. correspondent accounts
   - 320 - expands forfeiture for offenses against foreign nations
   - 323 - enforcement of foreign forfeiture judgments
   - 324 - expands geographic targeting orders
   - 359 - SARS
   - 363 - expands penalties for money laundering
   - 372 - criminal and civil forfeitures in currency-reporting cases
   - 374 - expands counterfeiting statute
   - 375 - expands penalty for counterfeiting foreign currency
   - 376 - material support included in money laundering
   - 377 - extra-territorial jurisdiction for fraud with (e.g.) credit card numbers
   - 1004 - expanded jurisdiction for money laundering

5. Visitor controls
    - 412 - AG required to detain aliens he certifies as threat to NS
    - 413 - share visa records with foreign governments
    - 416 - AG to expand foreign student visa monitoring

6. Expanded criminal statutes
    - 801 - attacks on mass transportation systems
    - 803 - criminalizes harboring of certain offenders
    - 804 - crimes at foreign missions
    - 805 - expanded "material support"
    - 806 - civil forfeiture of terrorist assets
    - 809 - eliminated statute of limitations for some offenses
    - 810 - enhanced penalties for certain crimes
    - 811 - attempt and conspiracy added
    - 814 - expanded jurisdiction for computer crimes
    - 817 - expanded biological weapons statute
    - 1011 - unlawful to fraudulently solicit charitable contribution

SUNSET PROVISIONS IN BOLD

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism. (1)

Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses. (1)

Sec. 203. Authority to share criminal investigative information.
203 (b) (Title III) and (d) (Grand Jury) (1)

Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications. (1)

Sec. 205. Employment of translators by the Federal Bureau of Investigation.

Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978. (1)

Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power. (2)

Sec. 208. Designation of judges.

Sec. 209. Seizure of voice-mail messages pursuant to warrants. (2)

Sec. 210. Scope of subpoenas for records of electronic communications.

Sec. 211. Clarification of scope.

Sec. 212. Emergency disclosure of electronic communications to protect life and limb. (1)

Sec. 213. Authority for delaying notice of the execution of a warrant.

Sec. 214. Pen register and trap and trace authority under FISA. (1)

Sec. 215. Access to records and other items under the Foreign Intelligence Surveillance Act. (1)

Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices.

Sec. 217. Interception of computer trespasser communications. (1)

Sec. 218. Foreign intelligence information. (1)

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 2
Page 7 ~ Duplicate
Page 8 ~ Duplicate

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

MUSLIM COMMUNITY ASSOCIATION OF ANN ARBOR; AMERICAN-ARAB ANTI-DISCRIMINATION COMMITTEE; ARAB COMMUNITY CENTER FOR ECONOMIC AND SOCIAL SERVICES; BRIDGE REFUGEE & SPONSORSHIP SERVICES, INC; COUNCIL ON AMERICAN-ISLAMIC RELATIONS; ISLAMIC CENTER OF PORTLAND, MASJED AS-SABER,

Plaintiffs,

v.

JOHN ASHCROFT, in his official capacity as Attorney General of the United States; ROBERT MUELLER, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Case No.

Hon.

ANN BEESON
JAMEEL JAFFER
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500

MICHAEL J. STEINBERG
NOEL SALEH
KARY L. MOSS
American Civil Liberties Union Fund of Michigan
60 West Hancock
Detroit, MI 48201-1343
(313) 578-6800

Attorneys for Plaintiffs.

COMPLAINT

PRELIMINARY STATEMENT

1. This lawsuit challenges the constitutionality of Section 215 of the USA PATRIOT Act, which vastly expands the power of the Federal Bureau of Investigation ("FBI") to obtain records and other "tangible things" of people not suspected of criminal activity. Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) ("Patriot Act" or "Act"). The FBI can use Section 215 to obtain personal belongings, including "books, records, papers, documents, and other items," directly from a person's home. It can also order charities, political organizations, libraries, hospitals, Internet Service Providers, or indeed *any* person or entity to turn over the records or personal belongings of others. The FBI can use Section 215 against anyone at all, including United States citizens and permanent residents.

2. Section 215 is invalid on its face. To obtain a Section 215 order, the FBI need only assert that the records or personal belongings are "sought for" an ongoing foreign intelligence, counterintelligence, or international terrorism investigation. The FBI is not required to show probable cause – or any reason – to believe that the target of the order is a criminal suspect or foreign agent. The FBI can obtain and execute Section 215 orders in total secrecy. The targets of Section 215 orders are *never* notified that their privacy has been compromised – even years later, and even if they are innocent. The law includes a gag provision that prohibits persons or entities served with Section 215 orders from ever disclosing, even in the most general terms, that the FBI has sought information from them. By seriously compromising the rights to privacy, free speech, and due process, Section 215 violates the First, Fourth, and Fifth Amendments of the United

States Constitution. Plaintiffs respectfully seek a declaration that Section 215 is facially unconstitutional, and a permanent injunction against its enforcement.

JURISDICTION AND VENUE

3. This case arises under the United States Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the United States Constitution and 28 U.S.C. § 1331. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*. The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412. Venue is proper in this district under 28 U.S.C. § 1391(e).

PARTIES

4. Plaintiff Muslim Community Association of Ann Arbor ("MCA") is a non-profit, membership-based organization that serves the religious needs of Muslims in and around Ann Arbor, Michigan. MCA owns and administers a mosque and an Islamic school. MCA sues on its own behalf and on behalf of its members, students, and constituents.

5. Plaintiff American-Arab Anti-Discrimination Committee ("ADC") is a non-profit civil rights organization committed to defending the rights of people of Arab descent and promoting their rich cultural heritage. ADC, which is non-sectarian and non-partisan, is the largest Arab-American grassroots organization in the United States. Based in Washington, D.C., it was founded in 1980 by former United States Senator James Abourezk and has chapters nationwide. ADC sues on its own behalf and on behalf of its members and constituents.

6. Plaintiff Arab Community Center for Economic and Social Services ("ACCESS") is a Detroit-based human services organization committed to the development of the Arab-American community in all aspects of its economic and cultural life. Among other services, ACCESS operates a Community Health and Research Center. ACCESS sues on its own behalf and on behalf of its members, clients, and constituents.

7. Plaintiff Bridge Refugee & Sponsorship Services, Inc. ("Bridge") is an ecumenical, non-profit organization based in Knoxville, Tennessee, dedicated to helping refugees and asylum-seekers become and stay self-sufficient. Bridge is affiliated with Church World Service and with Episcopal Migration Ministries. Bridge recruits and trains church sponsors to help refugees create new lives in East Tennessee, and provides services until refugees are eligible to apply for United States citizenship. Bridge sues on its own behalf and on behalf of its clients.

8. Plaintiff Council on American Islamic Relations ("CAIR") is a non-profit, mainstream, grassroots organization dedicated to enhancing the public's understanding of Islam and Muslims. CAIR is the largest Islamic civil liberties organization in the United States. CAIR is based in Washington, D.C., and has chapters nationwide and in Canada. CAIR sues on its own behalf and on behalf of its members and constituents.

9. Plaintiff Islamic Center of Portland, Masjed As-Saber ("ICPMA"), is a non-profit organization that serves the religious needs of Muslims in and around Portland, Oregon. ICPMA owns and administers a mosque known as Masjed As-Saber and an Islamic school known as the Islamic School of Portland. ICPMA sues on its own behalf and on behalf of its community members and students.

10. Defendant Attorney General John Ashcroft heads the United States Department of Justice, which is the agency of the United States government responsible for enforcement of federal criminal laws and domestic intelligence investigations. Defendant Attorney General Ashcroft has ultimate authority for supervising all of the operations and functions of the Department of Justice. The Department of Justice includes the FBI, the agency authorized to use the law challenged in this case.

11. Defendant Robert Mueller is the Director of the FBI, which is the principal investigative arm of the United States Department of Justice. Defendant Robert Mueller is responsible for supervising all of the operations and functions of the FBI. The FBI is the agency authorized to use the law challenged in this case.

STATUTORY LANGUAGE AT ISSUE

12. The Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, was enacted in 1978 to govern FBI surveillance of foreign powers and their agents inside the United States. *See* Pub. L. 95-511, 92 Stat. 1783 (Oct. 25, 1978). Through FISA, Congress created the Foreign Intelligence Surveillance Court ("FISA Court"), originally composed of seven (now eleven) federal district judges empowered to grant or deny government applications for FISA surveillance orders. *See* 50 U.S.C. § 1803.

13. Since 1978, Congress has amended FISA numerous times, each time adding new tools to the FBI's foreign intelligence toolbox or expanding the class of investigations in which such tools may be employed.

14. One amendment, which was codified as Subchapter IV of FISA, authorized the FBI to obtain "business records" from vehicle rental agencies, common carriers, storage facilities, and other similar businesses if the FBI had "specific and

articulable facts" giving reason to believe that the records in question pertained to a foreign agent or power. *See* Pub. L. 105-272, Title VI, § 602, 112 Stat. 2411 (Oct. 20, 1998).

15. The Patriot Act was passed on October 26, 2001.

16. Section 215 of the Patriot Act amended Subchapter IV of FISA by: (i) allowing the FBI to demand the production of "any tangible things (including books, records, papers, documents, and other items)," and not just business records; (ii) allowing the FBI to demand books, records and other tangible things from *anyone*, and not just from vehicle rental agencies and other third parties; and (iii) allowing the FBI to demand books, records and other tangible things without showing any evidence that the person whom it is investigating is a foreign agent. *See* 50 U.S.C. § 1861(a)(1).

17. Section 215 does not require the FBI to show probable cause or any reason to believe that the records or personal belongings sought pertain to a person involved in criminal activity or to a foreign agent or foreign power. *See id.* § 1861(b)(2). The provision requires only that the FBI certify to the FISA Court that the books, records, or other tangible things demanded on the authority of the provision are "sought for" a foreign intelligence, clandestine intelligence, or international terrorism investigation. As a result of the changes effected by the Patriot Act, the FBI is now authorized to use Section 215 even against people who are known to be altogether unconnected to criminal activity or espionage.

18. Section 215 requires the FISA Court to defer to the FBI's specification that the records or personal belongings sought by a Section 215 order are sought for an investigation to obtain foreign intelligence information or to protect against international

terrorism or clandestine intelligence activities. The FISA Court has no statutory authority to examine the foundation of the FBI's specification or to reject the specification as unfounded. *See id.* § 1861(b)(2) & (c)(1).

19. Section 215 does not require the FBI to have reason to believe that the records or personal belongings sought pertain to a particular suspect or a particular offense. Accordingly, the FBI could use Section 215 to obtain from a bookstore a list of people who had purchased a particular book, or to obtain from a health clinic a list of patients who had received medical care. The FBI need not state or even know in advance which individuals' privacy will be infringed.

20. At a hearing before the House Judiciary Committee on June 5, 2003, Defendant Attorney General John Ashcroft stated that, prior to the Patriot Act, the government "used to have [to allege] a reason to believe that the target is an agent of a foreign power," a standard he agreed was "lower than probable cause." He acknowledged that, under Section 215, the government may now obtain "all relevant, tangible items" without such a showing.

21. Section 215 does not require the FBI ever to notify surveillance targets that it has obtained their records or personal belongings.

22. Section 215 does not include any procedure that would allow a person or entity served with a Section 215 order to challenge the order's constitutionality before turning over the records or personal belongings sought by the order.

23. Section 215 authorizes the FBI to obtain records or personal belongings of United States citizens and permanent residents based in part on "activities protected by the first amendment to the Constitution." *Id.* § 1861(a)(1); *see also* § 1861(a)(2)(B).

24. Section 215 authorizes the FBI to obtain records or personal belongings of people who are not United States citizens or permanent residents based *solely* upon "activities protected by the First Amendment to the Constitution." *See id.* § 1861(a)(1); *see also* § 1861(a)(2)(B).

25. Section 215 requires the FISA Court to defer to the FBI's specification that the investigation is not being conducted of a United States person solely upon the basis of activities protected by the First Amendment. The FISA Court has no statutory authority to examine the foundation of the FBI's specification or to reject the specification as unfounded. *See id.* § 1861(b)(2) & (c)(1).

26. Section 215 includes the following gag provision: "No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section." *See id.* § 1861(d). Section 215 gag orders are indefinite, and do not require the FBI to make a showing that secrecy is necessary in any particular case.

27. Defendant Attorney General John Ashcroft has refused to disclose publicly even the most basic information about the FBI's use of Section 215. He has refused to say, for example, how many times the provision has been used to obtain information from public libraries, how many times it has been used to obtain information about United States citizens or permanent residents, and how many times it has been used in response to a person's engagement in activity protected by the First Amendment.

28. Through a request submitted under the Freedom of Information Act, the American Civil Liberties Union obtained heavily redacted documents that indicate that the FBI has already used Section 215.

29. At a June 2003 hearing, Defendant Attorney General Ashcroft informed the House Judiciary Committee that it is his position that Section 215 could be used to obtain, among other things, library and bookstore records, computer files, education records, and even genetic information.

FACTUAL BACKGROUND

30. Based on their personal experiences and the government's own actions, plaintiffs have a well-founded belief that they and their members, clients, and constituents (hereinafter "members and clients") have been or are currently the targets of investigations conducted under Section 215. Because Section 215 does not require the government to provide notice to surveillance targets, and because it strictly gags recipients from disclosing that the FBI has sought or obtained information from them, plaintiffs and other innocent targets of FBI surveillance have no way to know with certainty that their privacy has been compromised.

31. The FBI has already targeted plaintiffs, their members, and their clients in a number of ways.

32. The FBI has sought information directly from some of the plaintiffs about their members and clients.

33. The FBI has sought information from some of the plaintiffs' members and clients directly, either during visits to their homes and businesses, or through numerous

registration and interview programs directed at Muslims of Arab and South Asian descent.

34. Plaintiffs have many members and clients who were required to register under the National Security Entry-Exit Registration System (NSEERS), an INS program that thus far has been applied almost exclusively to nationals of predominantly Arab and Muslim countries. Many individuals who appeared in good faith for registration were then detained by the INS for alleged immigration violations. The FBI also interviewed many of plaintiffs' members and clients of Arab, Muslim, and South Asian descent in March 2002. Finally, the FBI interviewed many of plaintiffs' members and clients of Iraqi descent in March 2003, as part of "Operation Liberty Shield."

35. During these interviews, many members were questioned about their religious and political beliefs, activities, and associations. Some of plaintiffs' members expressed opposition to the war in Iraq, to United States support for Israeli policies, and to other aspects of United States foreign policy. Plaintiffs' members and clients believe that the FBI may have selected them for investigation under Section 215 because of information obtained during these interviews.

36. The Attorney General stated publicly in November 2002 that the Justice Department had a "previously undisclosed intelligence program involv[ing] tracking thousands of Iraqi citizens and Iraqi Americans with dual citizenship."

37. The FBI is currently investigating a number of charities suspected of providing material support to Foreign Terrorist Organizations. Some of plaintiffs' members and clients contributed financially to these charities before the charities were accused of having provided material support.

38. Some of the plaintiffs and their members and clients have direct contacts with people whom the INS detained and the FBI interrogated after September 11th. The FBI routinely interrogated INS detainees, asking questions not only about the detainees' own immigration status, political views, religious beliefs, and foreign connections but also about the political views, religious beliefs, and foreign connections of the detainees' friends and family members.

39. Many of plaintiffs' members and clients emigrated to the United States from countries the government has accused of sponsoring terrorism, such as Syria and Iraq. Defendant Mueller has stated publicly that a "substantial" number of persons are under constant surveillance, particularly in communities like New York and Detroit, where plaintiffs have thousands of Arab-American members and clients.

40. Many of the plaintiffs directly serve Muslim communities, or have significant numbers of members or clients who are Muslim. Two of the plaintiffs, the Muslim Community Association of Ann Arbor and the Islamic Center of Portland, Masjed As-Saber, operate mosques.

41. Section 215 has caused some of plaintiffs' members and clients to be inhibited from publicly expressing their political views, attending mosque and practicing their religion, participating in public debate, engaging in political activity, associating with legitimate political and religious organizations, donating money to legitimate charitable organizations, exercising candor in private conversations, researching sensitive political and religious topics, visiting particular websites, and otherwise engaging in activity that is protected by the First Amendment to the United States Constitution.

Muslim Community Association of Ann Arbor

42. MCA is a non-profit, membership-based organization that owns and administers a mosque and an Islamic school, the Michigan Islamic Academy, in Ann Arbor, Michigan. Approximately 1000 people attend services at the mosque each Friday; as many as 2500 attend services on religious holidays. MCA employs approximately 20 people and has about 700 registered, dues-paying members.

43. Approximately 200 students are enrolled at the Michigan Islamic Academy, which offers classes from pre-K through 11th grade. In addition to offering the standard academic curriculum used in the State of Michigan for public schools, the school offers classes in Arabic language, Quranic recitation and Islamic Studies. The mission of the school is to provide students with the basic knowledge required to preserve their Islamic heritage, religion and cultural identity.

44. MCA has spent a significant amount of time, staff resources, and funds discussing the impact of September 11th and the Patriot Act on the civil rights of Muslims. It sponsored civil rights forums on January 26, 2002; April 14, 2002; October 13, 2002; and March 12, 2003. Each of these forums addressed the impact of the Patriot Act. The MCA has also sponsored numerous rallies and fundraisers related to the Rabih Haddad case; at these events, the Patriot Act was almost always discussed.

45. Because of the relationship between MCA, its members and leaders, and persons and organizations investigated, questioned, detained, or arrested since September 11th, MCA reasonably believes that the FBI has used or is currently using Section 215 to obtain records or personal belongings about it and its members, students, and constituents.

46. For example, the MCA, its leadership, and its members have been associated with Rabih Haddad. Rabih Haddad is a 41-year-old native of Lebanon who came legally to the United States and lived until recently in Ann Arbor with his wife and four children. He was an active member of MCA and a volunteer teacher at MCA's Michigan Islamic Academy. In 1992, he co-founded the Global Relief Foundation, a humanitarian organization which the federal government has accused of having provided material support for terrorism. In December 2001, Mr. Haddad was arrested on immigration charges. Though never accused of threatening or harming anyone, Mr. Haddad was denied bond and held in solitary confinement for months with almost no access to his family or the outside world. The INS commenced removal proceedings against him based on visa violations, and the government attempted to close the INS hearings to the press and public. The ACLU, the Detroit Free Press, Representative John Conyers and others successfully sued to open the hearings. Mr. Haddad was ultimately imprisoned for approximately nineteen months, and deported to Lebanon in July 2003. He was never charged with any crime.

47. Some MCA members founded the Free Rabih Haddad Committee in December 2001. The Free Rabih Haddad Committee supported the Haddad family during Mr. Haddad's imprisonment, raised money to assist in his defense, organized public demonstrations in support of Mr. Haddad, and organized a letter-writing campaign. The Free Rabih Haddad Committee continues to educate the public about the government's treatment of Mr. Haddad. The MCA itself also held numerous fundraisers and public rallies to protest Mr. Haddad's detention.

48. Almost all meetings of the Free Rabih Haddad Committee were held at the MCA. During his detention, Mr. Haddad placed weekly telephone calls to the MCA in order to speak with MCA leaders and members.

49. The MCA, its leadership, and its members have also been associated with Dr. Sami Al-Arian. In October 2002, Dr. Sami Al-Arian spoke at the MCA mosque on the "Eroding Status of Our Civil Liberties." Dr. Al-Arian is a Kuwaiti-born former professor at the University of South Florida. He was indicted in the Middle District of Florida in February 2003 for allegedly aiding and abetting terrorism in the occupied West Bank. The federal government has introduced evidence in the case that they obtained through wiretaps authorized under another Patriot Act amendment to FISA. Dr. Al-Arian's daughter, Layla Al-Arian, spoke about her father's case at MCA's mosque in March 2003.

50. Other MCA members and leaders have been individually targeted for investigation by the FBI.

51. For example, MCA member Homam Albaroudi was born in Syria and came to the United States in 1987. He received a Masters in Engineering from Missouri State University and a Ph.D. in Engineering from Oregon State University. He is now a United States citizen. He is married to a United States citizen and has three children, all United States citizens. He works as an engineer for a Fortune 100 company.

52. Mr. Albaroudi has been an active member of MCA since 1999. He was a member of the Michigan Islamic Academy's board of directors for 3 years.

53. Mr. Albaroudi has also been a member of CAIR's Michigan chapter for approximately three years.

54. In 1993, Mr. Albaroudi co-founded the Islamic Assembly of North America ("IANA"), a non-profit organization dedicated to educating the public about Islam. While he was associated with the organization, IANA organized conferences, published religious books, and supplied Qurans to incarcerated Muslims. Mr. Albaroudi served as IANA's Executive Director from the organization's founding in 1996 until 1997, when he stepped down from his position and ended his association with IANA because of personal differences with other IANA leaders. The FBI raided IANA's offices in February 2003, seizing computers and taking photographs of books. The computers contained information about Mr. Albaroudi. FBI agents also questioned IANA associates and ex-employees about Mr. Albaroudi, notwithstanding that his association with IANA ended in 1997.

55. Mr. Albaroudi was also a founder of the Free Rabih Haddad Committee. Mr. Albaroudi convened the initial meeting of the Committee on the premises of the MCA.

56. Mr. Albaroudi has twice been contacted by the FBI. On the first occasion, which was approximately four years ago, Mr. Albaroudi was on an employment-related consulting assignment in Indiana when the FBI came looking for him at his home in Michigan. When the FBI discovered that Mr. Albaroudi was not at home, they left their cards with Mr. Albaroudi's wife, asking that Mr. Albaroudi contact them when he returned. Mr. Albaroudi did so. The FBI did not pursue efforts to speak with Mr. Albaroudi after he informed them that he did not feel comfortable speaking with them without an attorney present.

57. The FBI contacted Mr. Albaroudi again in or about March 2003. On this occasion, the FBI agents who contacted him said that they had not singled him out but rather were interviewing many people in the area to find out whether anyone had learned of conspiracies against the United States. Mr. Albaroudi explained to the FBI that he would have contacted them of his own accord if he had learned of conspiracies against the United States. The FBI then asked Mr. Albaroudi about another co-founder of IANA, who had recently been arrested for an overdraft check and then detained on immigration charges. The FBI did not pursue efforts to speak with Mr. Albaroudi after he informed them that he did not feel comfortable speaking with them without an attorney present.

58. Mr. Albaroudi reasonably believes that, because of his religion, his ethnicity, his place of birth, his earlier leadership role in IANA, his leadership role in the Free Rabih Haddad Committee, and his membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain his records and personal belongings.

59. MCA member Kristine Abouzahr was born in Lansing, Michigan in 1958. She is married and has five children, the eldest of whom is 21 and the youngest 9. Mrs. Abouzahr received a B.S. from Oklahoma State University in 1978 and an M.A. from Virginia Polytechnic Institute and State University in 1980. She moved to Michigan in 1986.

60. Mrs. Abouzahr has been a member of the MCA since 1986.

61. Mrs. Abouzahr taught at the Michigan Islamic Academy from 1990-1994, from 1995-1997, from 1999-2001, and during this past academic year. Mrs. Abouzahr's youngest daughter is currently a student at the Michigan Islamic Academy.

62. Mrs. Abouzahr serves on MCA's Outreach Committee, whose mandate is to educate Americans about Islam. As a member of the Outreach Committee, she has visited numerous local schools and community organizations to give presentations about Islam. Mrs. Abouzahr also serves informally as an advisor to Michigan Islamic Academy's new immigrant students and their parents who have questions about adjusting to life in the United States.

63. Mrs. Abouzahr is an active member of the Ann Arbor Area Committee for Peace (AAACP). As a member of that organization, Mrs. Abouzahr attended demonstrations against the Gulf War, against the Patriot Act, against the FBI's "voluntary" interview program, and in favor of a just peace between Israel and Palestine. Mrs. Abouzahr has also spoken publicly at demonstrations sponsored by AAACP and MCA, including at demonstrations in support of Rabih Haddad.

64. Mrs. Abouzahr is also an active member of the Free Rabih Haddad Committee. As one of the Committee's two Media Coordinators, she drafts press releases, speaks to the media, and organizes public demonstrations. She has also spoken publicly in support of Mr. Haddad. For example, in February 2002, after she had traveled to Washington, D.C., with Mr. Haddad's wife, she spoke at an informational forum organized and co-sponsored by the AAACP and the Free Rabih Haddad Committee to inform the local community about Haddad's case.

65. The Free Rabih Haddad Committee's post office box is registered in Mrs. Abouzahr's name.

66. Mrs. Abouzahr reasonably believes that, because of her religion, her leadership role in the Free Rabih Haddad Committee, her membership in AAACP, and

her membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain her records and personal belongings.

67. MCA member Nazih Hassan was born in Lebanon in 1969. He emigrated to Canada in 1988 and became a Canadian citizen in 1993. Mr. Hassan received his B.Esc. from the University of Western Ontario in 1994.

68. Mr. Hassan came to the United States in 1994 to study at Eastern Michigan University. He received his M.S. in Computer Information Systems from that institution in 1997.

69. Mr. Hassan became a legal permanent resident in 2001. He is married and has three children, two of whom are United States citizens. Mr. Hassan now works as a technology consultant and resides in Ypsilanti, Michigan.

70. Mr. Hassan has been a member of the MCA since 1994. Since January 2002, he has served as MCA's President. At various times since 1995, he also served as Editor of MCA's newsletter, as MCA's Secretary, and as MCA's Vice President.

71. Mr. Hassan was a founder of the Free Rabih Haddad Committee. As one of the Committee's two Media Coordinators, he drafts press releases, speaks to the media, and organizes public demonstrations.

72. Mr. Hassan reasonably believes that, because of his religion, his ethnicity, his place of birth, his leadership role in the Free Rabih Haddad Committee, and his membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain his records and personal belongings.

73. MCA also reasonably believes that it could be served with a Section 215 order. It then would have no ability to challenge the order before compromising the

privacy and free speech rights of its members. MCA maintains various records pertaining to its members, including records of members' names, telephone numbers, e-mail, home and business addresses, and citizenship status and national origin. MCA keeps records relating to members' marriages and divorces, and relating to members' family problems that MCA's Imam and Social Committee help resolve. MCA also keeps records documenting the use of zakat (members' charitable donations). The Michigan Islamic Academy also maintains a variety of educational and counseling records about its students. Finally, MCA has a variety of religious documents associated with the mosque and the Michigan Islamic Academy.

74. MCA has a policy of strictly maintaining the privacy of its records and routinely assures its members that any information they provide to MCA will be kept confidential. MCA's members rely on MCA's assurances that their records will be kept confidential.

75. Section 215 compromises MCA's ability to maintain the confidentiality of records pertaining to its members and students, and to protect individual members and students from harassment, threats, and violence. MCA has been the target of harassment since September 11th. For example, on some occasions after MCA President Nazih Hassan was quoted in newspaper articles, the MCA received several hate letters. After Mr. Hassan wrote a letter to the Ann Arbor News at the end of March 2003, an unknown individual or group placed hate fliers on cars outside the mosque. Were the confidentiality of MCA's records to be compromised and MCA's membership list to become public knowledge, MCA's individual members would be subjected to verbal harassment, threats, and even violence.

76. MCA's ability to keep its records confidential also allows MCA to protect its members and students from the possibility that the government will target them for their exercise of First Amendment rights, including their rights to free speech, free association, and free exercise of religion.

77. Because of the likelihood that the FBI is using provisions of the Patriot Act to target MCA, its leadership, and its members, some MCA members are afraid to attend mosque, to practice their religion, or to express their opinions about religious and political issues. Several people have told MCA leaders that they do not attend mosque for fear that the FBI is surveilling MCA and intends to investigate those who are associated with the organization.

American-Arab Anti-Discrimination Committee

78. ADC is a non-profit civil rights organization committed to defending the rights and promoting the rich cultural heritage of people of Arab descent. ADC has members and volunteer-based chapters in many states. It is headquartered in Washington, D.C., and has staffed offices in New York City, Detroit, San Diego, and San Francisco.

79. Since the passage of the Patriot Act, ADC has spent a significant amount of time, staff resources, and funds in advocating against the civil rights encroachments authorized by the Act. ADC has co-sponsored congressional briefings in Washington, D.C., and held town hall meetings throughout the country to educate the public about the Act. Most recently, ADC was a major co-sponsor of a national congressional briefing held on Capitol Hill on June 4, 2003. The briefing, which was attended by several prominent senators and representatives, featured testimony from immigrants who had

suffered civil rights violations after September 11th. On June 2, 2003, ADC co-sponsored another congressional staff briefing focusing on the Act and other post-September 11 Department of Justice initiatives. ADC staff members have spoken about the Patriot Act at over 150 conferences, seminars, and university events around the nation. Additionally, ADC's National Conventions for 2002 and 2003 included several panels discussing the Patriot Act and other government programs and policies implemented after the Patriot Act became law. ADC spokespeople, including Communications Director Hussein Ibish, are among the leading advocates in national media against the Patriot Act. Moreover, the ADC Legal Department provides routine assistance to anyone contacting ADC for help concerning law enforcement or other activities related to the Patriot Act. Finally, ADC's Legal Department is an active participant in coalition-based policy advocacy to amend or repeal parts of the Act.

80. ADC monitors the due process and equal protection rights of all Arab-Americans, including those who were detained on by the INS after September 11th and those who have been caught up in terrorism investigations.

81. For example, ADC and its members publicly condemned the use of secret evidence in the detention of Dr. Mazen Al-Najjar, formerly a University of South Florida professor. Though incarcerated for over three years, Dr. Al-Najjar was never charged with any criminal offense. He was ultimately deported for visa violations.

82. ADC and its members have also made public statements of concern about due process issues in the case of Rabih Haddad, a community leader in Ann Arbor, Michigan who was detained by the INS in December 2001, imprisoned for approximately

nineteen months, and ultimately deported in July 2003 without having been charged with any crime.

83. Because of the relationship between ADC, its members, and persons questioned, detained, or deported since September 11th, ADC reasonably believes that the FBI has used or is currently using Section 215 to obtain records and personal belongings about it and its members.

84. ADC also reasonably believes that it could be served with a Section 215 order. ADC would then would have no ability to challenge the order before compromising the privacy rights of its members. ADC maintains a variety of records about members, including their names and names of family members, home and business mailing addresses, phone numbers, email addresses, credit card information, and checking account information. ADC has a policy of maintaining the confidentiality of its members and their private information. ADC does not disclose membership numbers or any other information about members.

85. Section 215 compromises ADC's ability to maintain the confidentiality of records pertaining to its members, and to protect members from harassment, threats, and violence. ADC has documented a substantial increase in hate crimes, discrimination, and harassment against Arab-Americans since the September 11th attacks. Many of these incidents are described in the ADC publication, "Report on Hate Crimes and Discrimination Against Arab Americans; The Post-September 11 Backlash." Over 700 violent incidents occurred in the first nine weeks following the attack, including several murders. In the first year after the attacks, ADC documented over 80 cases in which airlines had discriminated against passengers who were perceived to be Arab. There

were also over 800 cases of employment discrimination against Arab-Americans, an approximately four-fold increase over previous annual rates, and numerous instances of denial of service, discriminatory service and housing discrimination. These numbers remain significantly above pre-September 11th levels today. Were the confidentiality of ADC's records to be compromised or ADC's full membership list to become public knowledge, ADC's members could risk harassment, threats, and even violence.

Arab Community Center for Economic and Social Services

86. ACCESS is a human services organization committed to the development of the Arab-American community in the United States. Its staff and volunteers serve low-income families, help newly arrived immigrants adapt to life in the United States, and educate Americans about Arab culture. ACCESS provides a wide range of social, mental health, educational, artistic, employment, legal and medical services. ACCESS has more than 2500 members and approximately 150 full-time staff.

87. ACCESS provides over seventy different programs to more than a hundred thousand people of all ethnic and religious backgrounds. In the last fiscal year, ACCESS provided more than 57,290 services in the area of social and legal services, more than 12,600 counseling and psychiatric services, more than 60,300 in health and health education services, and more than 55,600 employment and vocational services. ACCESS also provided more than 256,590 hours of educational and recreational services to youths and their parents, and sponsored cultural events and activities attended by many thousands of people.

88. For example, ACCESS runs a Community Health and Resources Center that offers a wide range of medical, public health, mental health and family counseling

services and programs. Its division of Psychosocial Rehabilitation for Survivors of Torture and Refugee Family Strengthening provides mental health services to torture victims and refugees. ACCESS also provides specialized services to victims of domestic violence, administers a breast and cervical cancer control program, and provides HIV/AIDS and STD education, counseling and testing. The Center's research division has twice sponsored a National Conference on Health Issues in the Arab Community.

89. ACCESS's Department of Social Services offers emergency food assistance, immigration services, and homelessness prevention programs. Its Department of Employment and Training offers a variety of job training programs, language instruction, and family acculturation services to help immigrants integrate into their new society. The Youth and Education Department provides after school homework assistance to students, special programs for at-risk youth, and recreation programs and teen dialogue opportunities for young people.

90. Because of the relationship between ACCESS, its members and clients, and persons questioned, detained, or deported since September 11th, ACCESS reasonably believes that the FBI has used or is currently using Section 215 to obtain records or other personal belongings about it and its members and clients.

91. Some of ACCESS's members and clients have been individually targeted for investigation by the FBI.

92. For example, ACCESS member Ahmad Ali Ghosn was born in Lebanon in 1965. He has been a legal permanent resident of the United States since 1993. Mr. Ghosn's application for naturalization has been pending for over seven years. Mr. Ghosn first submitted his application in June 1996. The INS later informed Mr. Ghosn that it

had lost the application and advised him to submit two duplicate applications. Mr. Ghosn did so. He received an acknowledgement notice from the INS in January 1998 – over five years ago. Since January 1998, the INS has required Mr. Ghosn to be fingerprinted on multiple occasions but it has never sought to schedule a naturalization interview.

93. The INS most recently required Mr. Ghosn to be fingerprinted in February 2002. When Mr. Ghosn appeared as he had been asked to, he was greeted not only by an INS criminal investigator but also by two FBI agents, who questioned him for over two hours about his associations with various individuals and charitable organizations in Lebanon. The FBI agents informed Mr. Ghosn that he could be naturalized if he cooperated with them, but that if he did not, his children would be seized by the government and placed in foster care. Mr. Ghosn answered the FBI's questions to the best of his ability but refused their request that he become an FBI or INS spy. He was not advised of his right to counsel.

94. Because of the FBI's actions, Mr. Ghosn reasonably believes that the FBI has used or is currently using Section 215 to obtain his records or other personal belongings.

95. ACCESS also reasonably believes that it could be served with a Section 215 order. It would then have no ability to challenge the order before compromising the privacy rights of its members and clients. ACCESS maintains a wide range of highly personal, sensitive records relating to the services it offers to clients. For example, the Community Health and Research Center maintains medical records for torture victims and refugees, and for breast cancer, mental health, and HIV/AIDS patients. It also

maintains files on domestic violence victims and family counseling clients. ACCESS routinely assures its clients that the information they provide will be kept confidential.

Bridge Refugee & Sponsorship Services

96. Bridge is an ecumenical, non-profit organization that helps refugees and asylum-seekers become and stay self-sufficient.

97. Bridge is affiliated with Church World Service ("CWS"), which is the relief, development, and refugee assistance ministry of 36 Protestant, Orthodox, and Anglican denominations in the United States, and with Episcopal Migration Ministries ("EMM"), which is the arm of the Episcopal Church that advocates for the protection of the refugees.

98. Bridge employs eight staff members and has offices in Knoxville, Chattanooga, and Bristol, Tennessee.

99. Bridge generally obtains clients in either of two ways. In some cases, a person residing in the United States asks Bridge to assist a relative whom the United States has granted refugee status but who has not yet arrived in the United States. In these cases (called "family reunification" cases), Bridge begins working with the refugee's family while the refugee is still outside the United States. In other cases, Bridge is assigned refugees' files by affiliate organizations such as CWS and EMM. These cases (called "free" cases) usually involve refugees who do not have family in the United States.

100. Historically, Bridge has served approximately 200 new refugees and asylum seekers in a year. Bridge's current caseload, which includes refugees who arrived in the United States over the last five years, includes approximately 500 files.

101. Bridge ordinarily serves its clients through individual sponsors, whom Bridge recruits from local churches, mosques, and synagogues.

102. Sponsors sign confidentiality agreements. Bridge staff explain and review the confidentiality agreement in sponsor training sessions.

103. Bridge provides its clients with a broad spectrum of resettlement services. For example, Bridge staff and sponsors ensure that new refugees have accommodations, furniture, clothing, and food; accompany new refugees to the Department of Health for medical examinations and immunizations; provide English language tutors to refugees who require them; ensure that refugee children enroll in school; provide cultural counseling to educate new refugees about American customs; assist new refugees in finding employment as quickly as possible; assist new refugees in complying with immigration requirements; assist refugees in applying for permanent residence and citizenship; direct refugees to social services provided by other organizations or by the federal and state governments; and counsel refugees about personal problems, including substance abuse, sexual abuse, discrimination at work or school, domestic violence, family planning, and divorce.

104. Bridge maintains various records pertaining to its clients, including records of clients' names, telephone numbers, and residential addresses. Bridge also keeps records of its clients' dates of arrival in the United States.

105. In many cases, Bridge's files also include case notes taken by Bridge staff. Case notes may document medical conditions from which the client has suffered in the past or that the client suffers currently. Case notes may also document the nature of the persecution that the client faced in her home country.

106. In some cases, clients consult Bridge staff about personal problems, including substance abuse, sexual abuse, discrimination at work or school, domestic violence, family planning, and divorce. In one case, for example, Bridge counseled a client about a venereal disease that she had acquired as a result of rape by a soldier. In another case, Bridge counseled an elderly client who was being mistreated by his daughters. Bridge's case notes include documentation of conversations relating to these and similarly intimate, personal problems.

107. In many cases, Bridge's refugee clients can obtain the assistance they need only from Bridge. There is no other resettlement services organization in East Tennessee whose staff have the relevant language and professional skills. When Bridge's clients decide that they cannot afford to entrust their personal information to Bridge, those clients generally do not obtain the help that they need from anywhere. They simply deal with their problems – including serious medical and personal problems – on their own.

108. Bridge is concerned that Section 215 compromises its ability to maintain the confidentiality of its clients' records. Bridge regularly assures its clients that the information they provide will be kept confidential, and explains that, under state law, the confidentiality of the information that clients provide is protected by a social worker privilege. Bridge provides its clients with a confidentiality agreement that assures clients that Bridge will disclose their records only "to facilitate the continuation of proper medical treatment and social services."

109. Bridge reasonably believes that it could be served with a Section 215 order. Bridge would then would have no ability to challenge the order before compromising the privacy rights of its members.

110. The FBI has approached Bridge for information about its clients on at least two occasions. In early November 2002, the FBI approached Bridge to ask it to disclose all records relating to its Iraqi-born clients. Bridge declined to disclose the records because the records included sensitive, personal information, including medical information.

111. On November 12, 2002, Bridge was served with a Subpoena To Testify Before Grand Jury, ordering the production of "Any and all records of Bridge . . . relating to any and all Iraqi-born people who have been assisted by Bridge Refugee and Sponsorship Services, Inc., including records that provide the name, address, telephone number, employer, and personal circumstances of such persons." Bridge moved to quash the subpoena but withdrew its motion when the FBI agreed not to seek more information than Bridge's clients would already have provided to the INS. The FBI made clear, however, that it might eventually demand more information. The FBI did not indicate what form such a demand might take.

112. Bridge client Muwafa Albaraqi was born in 1968 in Najaf, Iraq, where he lived until 1991. In 1991, at the encouragement of the United States, Mr. Albaraqi participated in an uprising against the government of Saddam Hussein. Although the uprising was successful in Najaf, American support did not materialize and ultimately the city fell again to the Iraqi Republican Guard. Those who had participated in the uprising were labeled traitors and were tortured, imprisoned, or killed. Mr. Albaraqi fled to Saudi Arabia.

113. Mr. Albaraqi lived in a United Nations-administered refugee camp in Saudi Arabia from March 1991 to September 1994. He applied for political asylum in the United States while living at the camp.

114. Mr. Albaraqi came to the United States in September 1994. His file, which was initially assigned to another refugee organization, was transferred to Bridge when Mr. Albaraqi decided that he would reside in Tennessee, where he had friends.

115. Bridge assisted Mr. Albaraqi in adjusting to life in Tennessee. For example, Bridge showed Mr. Albaraqi around Knoxville, pointing out where he could buy groceries and clothing, and showed him how to use the bus system. Bridge helped Mr. Albaraqi find a place to live, paid his first month's rent and utilities, and bought him groceries for his first week in the country. Bridge also helped Mr. Albaraqi apply for federal assistance, including food stamps and social security. Bridge accompanied Mr. Albaraqi to the Department of Health, where Mr. Albaraqi was given a medical examination and immunizations. Bridge also helped Mr. Albaraqi with his application for permanent residence and, eventually, his application for citizenship.

116. Mr. Albaraqi became a United States citizen in 1999. Mr. Albaraqi now works as a check-out clerk at a grocery store in Knoxville, Tennessee. He is also a part-time student in electrical engineering at the University of Tennessee.

117. The FBI came to Mr. Albaraqi's workplace in January 2003, stating that they wanted to talk to him. Mr. Albaraqi was not told that the interview was optional or voluntary or that he had a right to contact an attorney and have an attorney present at the interview.

118. During the interview, the FBI asked, among other questions, whether anyone associated with the Iraqi government had asked him to engage in terrorism against American targets; what he would do if an Iraqi agent asked him to engage in terrorism; and whether he might act differently if the Iraqi agent cut off his brother's finger and sent it to him in the mail.

119. Mr. Albaraqi would not have sought Bridge's assistance for sensitive, personal matters had he thought that the FBI could easily access Bridge's records under Section 215. Based on his own experience as a refugee, he believes that other refugees will be less likely to seek help from Bridge because the FBI can obtain their sensitive, personal records even when they have done nothing wrong.

Council on American-Islamic Relations

120. CAIR is a non-profit grassroots organization dedicated to enhancing the public's understanding of Islam and Muslims. CAIR is the largest Islamic civil liberties organization in the United States. CAIR's national office in Washington, D.C., has a permanent staff of about 25 people. Approximately the same number of people are employed by CAIR's state and local chapters.

121. Since the passage of the Patriot Act, CAIR has spent a significant amount of time, staff resources, and funds in advocating against the civil rights encroachments authorized by the Act. CAIR hosts an annual conference each March. At both the 2002 and 2003 conferences, multiple speakers explained the Patriot Act and discussed its import for Muslims in the United States. CAIR hosts an annual dinner each October. At both the 2001 and 2002 dinners, speakers explained the Patriot Act and discussed its import for Muslims in the United States. CAIR regularly distributes e-mail "Action

Alerts" to members and others who have subscribed to CAIR's Action Alert list. Since the Patriot Act became law, CAIR has distributed numerous Action Alerts related to the Patriot Act. CAIR has also issued numerous news releases related to the Patriot Act.

122. CAIR monitors the due process and equal protection rights of all Muslims living in the United States, including those detained on immigration charges after September 11th and those caught up in terrorism investigations. In 2002, CAIR issued a 54-page "Civil Rights Report" that, among other things, examined the impact that "anti-terrorism" policies, including the Patriot Act, had had on the civil liberties of American Muslims. CAIR issued a similar Civil Rights Report in 2001 and issued a new Civil Rights Report in July 2003.

123. Because of the relationship between CAIR, its members, and persons questioned, detained, or deported since September 11th, CAIR reasonably believes that the FBI is currently using Section 215 to obtain records and personal belongings of CAIR and its members.

124. For example, CAIR member Magda Bayoumi was born in Cairo, Egypt, in 1956. She came to the United States in 1977 and became a United States citizen in 1988. Mrs. Bayoumi has been a member of CAIR for approximately four years.

125. Mrs. Bayoumi is married and has three children, of whom the youngest is 10 and the eldest 17. Mrs. Bayoumi's husband was also born in Cairo, Egypt. He became a United States citizen in 1991. All of Mrs. Bayoumi's children are United States citizens. Mrs. Bayoumi and her family live in Syracuse, New York.

126. Mrs. Bayoumi works as a volunteer for several community organizations. She currently chairs the board of the Parents Advisory Group for the Special-Education

Director of the Syracuse School District. She serves as a board member of the Central New York Parent's Coalition for Children With Special Needs. She co-founded and serves on the board of the of Autism Support Group. She founded and serves on the board of the Ed Smith School's Support Group for Children With Special Needs.

127. Mrs. Bayoumi and her husband co-founded and serve on the board of the Central New York Chapter of the American Muslim Council, an organization that was established in 1990 to increase the effective participation of American Muslims in the political process.

128. Two FBI agents came to Mrs. Bayoumi's home on February 26, 2003. They first informed Mrs. Bayoumi that they wanted to question her husband. When Ms. Bayoumi told the agents that her husband was not at home, however, they began to question her instead.

129. The FBI's questioning focused on a donation that Mrs. Bayoumi and her husband had made to a charity called Help the Needy. Mrs. Bayoumi and her husband had donated several hundred dollars to the organization the previous year.

130. The agents asked Mrs. Bayoumi how much money she and her husband had contributed to the charity, whether she had attended a dinner that Help the Needy had recently hosted, whether she knew what the donation was being used for, and whether she would be upset if the money had been used to build a mosque. Mrs. Bayoumi told the FBI that she and her husband had donated a few hundred dollars to the charity in each of the previous few years, had attended the recent dinner, and had assumed that the donation would be used to provide food and medicine for needy people in Iraq.

131. The FBI did not inform Mrs. Bayoumi how they had learned that she and her husband had made a donation to Help the Needy.

132. On the same day that the FBI questioned Mrs. Bayoumi, the Department of Justice announced that a federal grand jury in Syracuse, New York, had returned an indictment charging Help the Needy and four individuals associated with it of transferring funds to persons in Iraq without having obtained the proper license. While Help the Needy was not accused of having providing anything other than humanitarian aid to people living in Iraq, the Justice Department's press release accused Help the Needy of attempting to undermine the President's efforts "to end Saddam Hussein's tyranny and support for terror."

133. Mrs. Bayoumi reasonably believes that because of her religion, her ethnicity, and her earlier support for Help the Needy, the FBI has used and is currently using Section 215 to obtain her records and other personal belongings.

134. CAIR also reasonably believes that it could be served with a Section 215 order. CAIR would then would have no ability to challenge the order before compromising the privacy rights of its members. CAIR maintains a variety of records about members, including their names, home and business mailing addresses, phone numbers, email addresses, credit card information, and checking account information. CAIR has a policy of maintaining the confidentiality of its members and their private information. CAIR does not disclose membership numbers or any other information about individual members.

135. Section 215 compromises CAIR's ability to maintain the confidentiality of records pertaining to its members, and to protect members from harassment, threats, and

violence. CAIR has documented a substantial increase in hate crimes, discrimination, and harassment against Muslim and Arab-Americans since the September 11th attacks. Many of these incidents are described in CAIR's 2001, 2002, and 2003 Civil Rights Reports. Were the confidentiality of CAIR's records to be compromised and CAIR's membership list to become public knowledge, CAIR members could risk harassment, threats, and even violence.

Islamic Center of Portland, Masjed As-Saber

136. The Islamic Center of Portland, Masjed As-Saber ("ICPMA"), is a non-profit organization that owns and administers a mosque known as Masjed As-Saber and an Islamic school known as the Islamic School of Portland. Approximately 450 people attend services at the mosque each Friday; as many as 3500 attend services on religious holidays. ICPMA employs approximately 16 people. Approximately 60 students are enrolled at the school.

137. Because of the relationship between ICPMA, its community members and leaders, and persons and organizations investigated, questioned, detained, or arrested since September 11th, ICPMA reasonably believes that the FBI has used or is currently using Section 215 to obtain records and personal belongings pertaining to it and its community members and students.

138. Some ICPMA community members have been individually targeted for investigation by the FBI.

139. In October, 2002, a federal grand jury in the District of Oregon indicted six individuals and charged them with various counts of conspiracy to wage war against the United States and to provide material support to Al Qaeda; a seventh individual was

indicted on similar charges in April 2003. A trial is currently scheduled for January 2004 in this case, which is known as the "Portland 7" case. Some of the defendants, Jeffrey Leon Battle, Patrice Lumumba Ford, and Habis Abdulla al Saoub, attended the ICPMA. In an affidavit submitted in support of the indictment of the defendants, Police Officer Thomas W. McCartney stated that a wired informant recorded conversations inside the Islamic Center of Portland, Masjed As-Saber, on June 6, 2002. The electronic surveillance was authorized under another Patriot Act amendment to FISA. The affidavit also states that the government obtained a number of records relating to the investigation. The affidavit does not state the legal authority utilized in obtaining these records. The government has stated publicly that the investigation into the alleged conspiracies is ongoing.

140. The FBI has also sought records from ICPMA. In March 2003, the ICPMA was served with a subpoena seeking financial records related to the defendants and their spouses in the Portland 7 case. ICPMA retained lawyers who moved to quash the subpoena because of the impact on the privacy rights of ICPMA's constituents, but was ultimately required to disclose the records. Some of ICPMA's constituents are now afraid to donate to ICPMA because they fear their donations will provoke FBI investigation and harassment. The FBI has also served subpoenas to over 25 people in the Portland area, some of whom attend ICPMA and other local mosques. The FBI has interviewed some ICPMA community members and has asked questions about other worshipers and their political and religious views.

141. In addition, some of ICPMA's leaders appear to be under investigation by the FBI but have not been charged with any crime.

142. For example, ICPMA president Alaa Abunijem was born in Saudi Arabia and came to the United States in 1989. He became a U.S. citizen in 1996. Mr. Abunijem is married to a U.S. citizen and has four children. He holds a B.S. degree in Electrical Engineering and an M.S. in Engineering and Technology Management. He currently works as an engineer for a Fortune 100 company, and has lived in Portland, Oregon, since 1999.

143. On December 17, 2002, Mr. Abunijem was stopped at the Seattle airport by U.S. Customs and questioned by both U.S. customs and FBI officials regarding the purpose of his trip to Saudi Arabia. The officials searched his documents, business cards, and credit cards for thirty minutes before returning them to him. On his return from Saudi Arabia on January 9, 2003, his luggage and documents were searched for over an hour and a half, and he was questioned by officials about his trip.

144. On February 26, 2003, an FBI agent called Mr. Abunijem at his work place and questioned him about a donation he had made to a charity called Help the Needy. Mr. Abunijem had made donations of several hundred dollars to the organization over the past few years. The FBI did not inform Mr. Abunijem how they had learned that he made a donation to Help the Needy. Mr. Abunijem told the FBI agent that he did not feel comfortable talking to the FBI without a lawyer.

145. On the same day that the FBI questioned Mr. Abunijem, the Department of Justice announced that a federal grand jury in Syracuse, New York, had returned an indictment charging Help the Needy and four individuals associated with it of transferring funds to persons in Iraq without having obtained the proper license. While Help the Needy was not accused of having providing anything other than humanitarian

aid to people living in Iraq, the Justice Department's press release accused Help the Needy of attempting to undermine the President's efforts "to end Saddam Hussein's tyranny and support for terror."

146. Since 1999, Mr. Abunijem has served as a board member of the Islamic Assembly of North America ("IANA"), a non-profit organization dedicated to educating the public about Islam. IANA organizes conferences, publishes religious books, and supplies Qurans to incarcerated Muslims. The FBI raided IANA's offices in Michigan in or about February 2003, seizing computers and taking photographs of books. The computers contained information about Mr. Abunijem. The government has not charged IANA with any crime, but has arrested one of the organization's former presidents, Bassem K. Khafagi, on federal bank fraud charges. Assistant U.S. Attorney Terry Derden of Boise, Idaho has stated publicly that "the investigation could expand to other directors and Islamic Assembly employees."

147. Mr. Abunijem has not been charged with any crime and strongly maintains his innocence.

148. Mr. Abunijem reasonably believes that because of his religion, his ethnicity, his place of birth, his leadership role in ICPMA and IANA, and his donations to Help the Needy, the FBI is currently using Section 215 to obtain his records and personal belongings.

149. ICPMA reasonably believes that it could be served with a Section 215 order. It would then have no ability to challenge the order before compromising the privacy rights of its members. ICPMA maintains a variety of records about community members, including their names and the names of family members, home and business

mailing addresses, phone numbers, email addresses, credit card information, and checking account information. ICPMA also retains records of services it provides to community members, including Islamic marriage contracts, and records of divorce proceedings and financial assistance given to needy families. The Islamic School of Portland retains health, financial and educational records pertaining to all of its students and staff. ICPMA has a policy of maintaining the confidentiality of all records pertaining to its community members, staff and students.

150. Section 215 compromises ICPMA's ability to maintain the confidentiality of its records, and to protect community members and students from harassment, threats, and violence. Since the September 11th attacks, ICPMA community members and other Arab-Americans have repeatedly been the target of harassment. Were the confidentiality of ICPMA's records to be compromised and ICPMA's community list or other records to become public knowledge, ICPMA's community members and students could risk verbal harassment, threats, and even violence.

151. ICPMA's ability to keep its records confidential also allows ICPMA to protect its community members from the possibility that the government will target them for their association with ICPMA, including their rights to free speech, free association, and free exercise of religion.

152. Because ICPMA community members believe that the FBI is currently using provisions of the Patriot Act to target ICPMA, and because the FBI has recorded conversations and services inside the mosque and sought records from ICPMA, many ICPMA community members are afraid to attend mosque, practice their religion, or express their opinions about religious and political issues.

CAUSES OF ACTION

153. Section 215 violates the Fourth Amendment by authorizing the FBI to execute searches without criminal or foreign intelligence probable cause.

154. Section 215 violates the Fourth Amendment by authorizing the FBI to execute searches without providing targeted individuals with notice or an opportunity to be heard.

155. Section 215 violates the Fifth Amendment by authorizing the FBI to deprive individuals of property without due process.

156. Section 215 violates the First Amendment by categorically and permanently prohibiting any person from disclosing to any other person that the FBI has sought records or personal belongings.

157. Section 215 violates the First Amendment by authorizing the FBI to investigate individuals based on their exercise of First Amendment rights, including the rights of free expression, free association, and free exercise of religion.

PRAYER FOR RELIEF

WHEREFORE Plaintiff respectfully requests that the Court:

1. Declare that Section 215 is unconstitutional under the First, Fourth, and Fifth Amendments.
2. Permanently enjoin Defendants from using Section 215.
3. Award Plaintiff fees and costs pursuant to 28 U.S.C. § 2412.
4. Grant such other and further relief as the Court deems just and proper.

Respectfully submitted,

ANN BEESON
JAMEEL JAFFER
National Legal Department
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500

MICHAEL J. STEINBERG
NOEL SALEH
KARY L. MOSS
American Civil Liberties Union Fund
of Michigan
60 West Hancock
Detroit, MI 48201-1343
(313) 578-6800

Dated: July 30, 2003

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 23
Page 2 ~ b1
Page 3 ~ b1
Page 4 ~ b1
Page 5 ~ b1
Page 6 ~ b1
Page 7 ~ b1
Page 8 ~ b1
Page 9 ~ b1
Page 10 ~ b1
Page 11 ~ b1
Page 12 ~ b1
Page 13 ~ b1
Page 14 ~ b1
Page 15 ~ b1
Page 16 ~ b1
Page 17 ~ b1
Page 18 ~ b1
Page 82 ~ Referral/Direct
Page 83 ~ Referral/Direct
Page 84 ~ Referral/Direct
Page 85 ~ Referral/Direct
Page 86 ~ Referral/Direct
Page 87 ~ Referral/Direct

(Rev. 08-28-2000) # 05-CV-0845

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-15-2005 BY 65179 DMH / JHF

Precedence: IMMEDIATE **Date:** 06/19/02

To: All Divisions **Attn:** Assistant Director;
SAC;
Legat
CDC

From: Office of the General Counsel
Investigative Law Unit, Room 7326
Contact: Investigative Law Unit, [redacted] b2

Approved By: Parkinson Larry R
Steele Charles M
[redacted] b6

Drafted By: [redacted] b7C

Case ID #: 66F-HQ- 1085160(Pending)

Title: NEW LEGISLATION
PATRIOT ACT OF 2001
PROVISIONS ADDRESSING INVESTIGATIVE ISSUES

Synopsis: To supplement guidance previously provided on the USA PATRIOT ACT of 2001 by highlighting provisions of the USA PATRIOT Act of 2001 which are of the most immediate interest to FBI investigations.

Reference: 66F-HQ-A1247863 Serial 70
66F-HQ-A1247863 Serial 71
66F-HQ-A1323588 Serial 364

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (otherwise referred to as the "USA PATRIOT Act" or "Patriot Act") which enhances many investigative tools available to the FBI. Over the last several months, the Office of the General Counsel (OGC) has provided guidance to the field on this Act in the form of e-mails, ECs, and presentations/training. Among the documents provided are a detailed section-by-

section analysis of certain provisions of the Act;[1] two separate ECs prepared by OGC's National Security Law Unit, dated October 26, 2001, entitled "NEW LEGISLATION, REVISIONS TO FCI/IT LEGAL AUTHORITIES, FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)" and "NEW LEGISLATION, REVISIONS TO FBI/IT LEGAL AUTHORITIES, NATIONAL SECURITY LETTERS"; and an EC prepared by OGC's Legal Forfeiture Unit, dated January 11, 2002, entitled "ASSET FORFEITURE MATTER." The purpose of this communication is to consolidate into one document the guidance previously provided and to highlight those provisions of the Patriot Act of greatest interest to FBI investigative efforts.

This EC has been broken down into three sections. Section I, Investigative Tools, addresses the provisions which modify, amend, or create investigative tools which may apply to many types of investigations. Section II, Money Laundering, highlights some of the new crimes and investigative tools aimed at the financial networks of criminal enterprises. The International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 was incorporated into the Patriot Act and was intended to significantly increase the United States' ability to combat the financing of terrorism. This section of the EC is only intended to summarize some of the highlights of the Act. Additional, more comprehensive guidance will be forthcoming. Section III, New Terrorism Offenses, summarizes some of the important changes in the criminal statutes regarding terrorist offenses. The forfeiture provisions, information sharing provisions, and other national security related provisions were addressed in detail in the aforementioned ECs and therefore will not be covered by this EC.

Many of the investigative tools provided in the Patriot Act are governed by a sunset provision which will result in their expiration on December 31, 2005 unless renewed by Congress.[2] In order to be prepared to justify their renewal, offices are encouraged to keep records of the effective use of these tools. Important information to be maintained includes both the number of times the investigative tool was effectively used and specific information on noteworthy cases.

---

[1]This document was prepared by the Department of Justice and provided via e-mail to all Chief Division Counsels on October 30, 2001.

[2]Title 3 of the Patriot Act, entitled the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, has a slightly different sunset provision in that it will only expire if Congress enacts a joint resolution containing specific language. The result is that the provisions will continue unless Congress acts otherwise.

I. Investigative Tools

Information from Communications Providers

Voice Mail - Law enforcement can now obtain all voice mail which is stored by a communications provider, including unopened voice mail, using the procedures set forth in 18 U.S.C. §2703 (such as a search warrant). This also applies to other wire communications as defined by the statute. Voice messages stored and in the possession of the user, such as an answering machine, are not covered by this statute. [redacted] This tool is set to expire under the sunset provision. See 18 U.S.C. § 2510; 18 U.S.C. § 2703. b5

Basic Subscriber Information - The list of information law enforcement can obtain with a subpoena was expanded to include records of session times and durations, any temporarily assigned network address, and the means and source of payment that a customer uses to pay for his/her account with a communications provider. 18 U.S.C. § 2703(c).

Nationwide Search Warrants for E-mail - Courts with jurisdiction over an investigation can now issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. This tool is set to expire under the sunset provision. 18 U.S.C. § 2703.

Clarification of the Cable Act - In the past there were two statutory standards for privacy protection: one governing cable service (47 U.S.C. § 551, the "Cable Service Act"), and the other governing telephone and Internet privacy (18 U.S.C. § 2510, *et seq.* [wiretap statute], 18 U.S.C. § 2701, *et seq.* [ECPA], 18 U.S.C. § 3121 *et seq.* [pen/trap statute]). This opened the door for cable companies which provide telephone and Internet services to argue that the ECPA, wiretap, and pen/trap statutes did not apply to them. The Patriot Act clarified this issue by stating that the ECPA, wiretap, and pen/trap statutes govern disclosures by cable companies that relate to the provision of communication services. See 47 U.S.C. § 551(c)(2)(D).

Voluntary Disclosures - The law now explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers. The Act also allows a communications service provider to disclose non-content records to protect their rights and property. This will most often be used when the communications service provider itself is a victim of computer

hacking. This provision will expire under the sunset provision. See 18 U.S.C. § 2702(b) & (c)(3); 18 U.S.C. § 2703(c)(2)(F).

Electronic Surveillance

Expanded Predicates for Title III - The predicate offenses for Title III were expanded to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). This is set to expire under the sunset provision. See 18 U.S.C. § 2516.

Nationwide Effect of Pen/Trap Orders - The Act amends the pen/trap statute to give federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order. See 18 U.S.C. § 3127(2).

For example, a federal prosecutor may obtain an order to trace calls made to a telephone within the prosecutor's local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the investigators may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path to convey to the next carrier in the chain. The investigator would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order had been served on the originating carrier who was able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider. OGC will provide additional guidance on language for such certification in the near future.

Intercepting Communications of Computer Trespassers - The wiretap statute was amended to explicitly rovide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and

intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer. Additionally, based on the definition of a "computer trespasser," communications of users who have a contractual relationship with the computer owner may not be monitored, even if their use is in violation of their contract terms (i.e. spammers). This is set to expire under the sunset provision. See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

Pen Register/Trap and Trace Reporting Requirement - The statute created a new reporting requirement whenever the government uses its own pen register or trap and trace equipment on a packet-switched data network of an electronic communications service to the public. While this provision was aimed at the use of the DCS-1000 (earlier versions were known as Carnivore), it will also apply to the use of other government owned equipment/software, such as Etherpeek, on a service provider's network. While additional detailed guidance will be forthcoming, this new requirement imposes a duty to maintain records relating to the use of this equipment and to file these records with the court which authorized the pen register or trap and trace. See 18 U.S.C. § 3123(a)(3).

OPR Inquiry and Civil Liability for Unauthorized Disclosures - If a court, appropriate department, or agency, 1) finds that the government violated the wiretap statute (18 U.S.C. § 2520, *et seq.*) or the Electronic Communications Privacy Act (ECPA codified at 18 U.S.C. § 2701, *et seq.*); and 2) seriously questions if a government employee acted willfully or intentionally in such violation, the statute now requires that an OPR inquiry be initiated to determine if disciplinary action is warranted. The Department of Justice Inspector General will be notified of the results of the inquiry, including justification for the outcome. Violations warranting an OPR inquiry include improper disclosure of information obtained pursuant to Title III, ECPA, a pen register/trap and trace order, and national security letters under 18 U.S.C. § 2709. The United States is now civilly liable for certain violations of FISA [Section 106(a) codified at 50 U.S.C. § 1806(a) (the use of information in the ELSUR context), Section 305(a) codified at 50 U.S.C. § 1825(a) (the use of information in the physical search context), and Section 405(a) codified at 50 U.S.C. § 1845(a) (the use of information in the pen register/trap and trace context)], the wiretap statute, and ECPA with minimum damages awarded at $10,000 plus legal fees. See 18 U.S.C. § 2520(f) & (g); 18 U.S.C. § 2707(d) & (g); and 18 U.S.C. § 2712.

Search Warrants

Delayed Notice for Search Warrants - The Act created a uniform statutory standard authorizing courts to delay the provision of required notice if the court finds "reasonable cause" to believe that providing immediate notification of the execution of the warrant may have an adverse result as defined by 18 U.S.C. § 2705 (including endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation or unduly delaying a trial). The Act provides for the giving of notice within a "reasonable period" of a warrant's execution, which period can be further extended by a court for good cause. See 18 U.S.C. § 3103a.

Single Jurisdiction Search Warrants for Terrorism - In domestic terrorism (as defined within the act) or international terrorism cases, a search warrant may be issued by a magistrate judge in any district in which activities related to the terrorism have occurred for a search of property or persons located within or outside of the district. See Fed. R. Crim. P. 41(a). U.S. Attorneys' Offices had been advised to coordinate all search warrants in the investigation into the September 11 terrorist attacks with the DOJ Terrorism and Violent Crimes Section in order to avoid duplication of effort and prevent inadvertent interference with ongoing investigations in another district. b5

Miscellaneous Tools

Obtaining Financial Records and Consumer Reports - Section 358 of the Act amended the Right to Financial Privacy Act and the Fair Credit Reporting Act to provide for the ability to obtain financial records or consumer reports related to "intelligence or counterintelligence activity, investigation or analysis related to international terrorism." See 31 U.S.C. § 5311; 12 U.S.C. § 3412(a).

DNA Predicates - Section 503 extends DNA sample collection to all federal offenders convicted of the types of offenses that are likely to be committed by terrorists (as set forth in 18 U.S.C. § 2332b(g)(5)(B)) or any crime of violence (as defined in 18 U.S.C. §16). See 42 U.S.C. §14135a(d)(2).

Emergency Assistance from DOD - The Act broadened the Attorney General's authority to request assistance from the Secretary of Defense in emergency situations involving weapons of mass destruction. See 18 U.S.C. § 2332e.

Educational Records - Law enforcement can now obtain educational records held by an educational agency or institution if they are relevant to an authorized investigation of domestic or international terrorism or other offenses found under 18 U.S.C. § 2332b(g)(5)(B).

Assistant Attorney General approval is required. This includes individually identifiable information which may be in the possession of the National Center for Education Statistics. See 20 U.S.C. § 1232g; 20 U.S.C. § 9007.

Expanded Foreign Jurisdiction - The special maritime and territorial jurisdiction of the United States explicitly is extended to U.S. diplomatic and consular premises and related private residences overseas for offenses committed by or against a U.S. national. This clarified inconsistent prior caselaw to establish that the United States may prosecute offenses committed in its missions abroad, by or against its nationals. The provision explicitly exempts offenses committed by members or employees of the U.S. armed forces and persons accompanying the armed forces, who are covered under a provision of existing law, 18 U.S.C. § 3261(a). See 18 U.S.C. § 7.

Expansion of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) - The Act included a variety of modifications to strength the criminal statute used most often in computer hacking cases (18 U.S.C. § 1030). The Patriot Act increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a particular *type* of damage; adds a new offense for damaging computers used for national security or criminal justice purposes; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for the purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold. See 18 U.S.C. § 1030.

II. Money Laundering

New Offenses

Bulk Cash Smuggling - The Act makes it an offense to smuggle more than $10,000 in currency into or out of the United States with the intent to evade the CMIR reporting requirement. The House Report specifically states that this provision will apply to conduct occurring before the effective date of the Act. 31 U.S.C. § 5332.

Money Transmitting Businesses - The scope of 18 U.S.C. § 1960 is expanded to include any business, licensed or unlicensed, that involves the movement of funds that the defendant knows were derived from a criminal offense, or were intended to be used "to promote or support unlawful activity."

b5

It is already an offense under Sections 1956 and 1957 for any person to conduct a financial transaction involving criminally derived property. But Section 1957 has a $10,000 threshold requirement, and Section 1956 requires proof of specific intent either to promote another offense or to conceal or disguise the criminal proceeds. New Section 1960 contains neither of these requirements if the property is criminal proceeds; or alternatively, if there is proof that the purpose of the financial transaction was to commit another offense, it does not require proof that the transmitted funds were tainted by any prior misconduct. See 18 U.S.C. § 1960.

New Investigative Tools

Expansion of Money Laundering Predicates - The list of foreign crimes in the definition of "specified unlawful activity" is expanded to include public corruption and other foreign offenses. Similarly, amendment to RICO makes a long list of acts relating to terrorism predicates for money laundering. Moreover, under Section 1956(a)(2)(A), it will be an offense to send any money from any source into or out of the United States with the intent to promote such an offense.

Subpoenas for Overseas Bank Records - A new statute, 31 U.S.C. § 5318(k)(3), provides that the Attorney General or the Secretary of the Treasury may serve "a summons or subpoena" on any foreign bank that has a correspondent account in the United States, and request records relating to that correspondent account or any records maintained outside of the United States relating to the deposit of funds into the foreign bank. Congress has created this authority by requiring that any foreign bank that maintains a correspondent account in the United States must appoint a representative to accept a subpoena issued by the Attorney General or the Secretary of the Treasury for bank records. [redacted] b5 This section of the Act became effective on December 25, 2001.

Long-Arm Jurisdiction - The Act expanded the court's jurisdiction to include a foreign person, including a foreign bank, if the money laundering offense occurred in part in the United States, or the foreign bank has a correspondent account in the United States. See 18 U.S.C. § 1956(b).

Voluntary Disclosure by Banks - The Act provides immunity from civil liability for any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency. It further prohibits, with some limited exceptions, the person or entity making such disclosure from notifying the person involved in the suspicious transaction that the transaction has been reported. See 31 U.S.C. § 5318(g)(3).

III. New Terrorism Offenses

Definitions

Domestic Terrorism - The Act created a new definition of "domestic terrorism," corresponding to the existing definition of "international terrorism." The term is defined to mean activities occurring primarily within the territorial jurisdiction of the United States involving acts dangerous to human life that are a violation of the criminal laws of the United States or any state and appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnaping. Investigations of "domestic terrorism" and "international terrorism" have additional investigative tools including nationwide service of search warrants and disclosure of educational records. See 18 U.S.C. § 2331; Fed. R. Crim. P. 41(a); 20 U.S.C. § 1232g; 20 U.S.C. § 9007.

Federal Crime of Terrorism (18 U.S.C. § 2332b(g)(5))- The definition was modified to include several offenses likely to be committed by terrorists, including a number of aircraft violence crimes and certain computer crimes, to the list of predicate offenses. Due to Congressional concerns about overbreadth, some crimes were removed from the list (primarily offenses involving assault and less grave property crimes). These offenses are now RICO predicates (see USA Patriot Act § 813), have a longer or no statute of limitations (18 U.S.C. § 3286), and are predicates for the collection of DNA (see Section I. above).

New Offenses

Attacks on Mass Transportation Systems - The law now prohibits various violent offenses against mass transportation systems, vehicles, facilities, or passengers. Specifically, it prohibits disabling or wrecking a mass transportation vehicle; placing a biological agent or destructive substance or device in a mass transportation vehicle with intent to endanger safety or with reckless disregard for human life; setting fire to or placing a biological agent or destructive substance or device in a mass transportation facility knowing or having reason to know that the activity is likely to disable or wreck a mass transportation vehicle; disabling mass transportation signaling systems; interfering with personnel with intent to endanger safety or with reckless disregard for human life; use of a dangerous weapon with intent to cause death or serious bodily injury to a person on the property of a mass transportation provider; conveying false information about any such offense; and attempt and conspiracy. The provision carries a maximum sentence of 20 years imprisonment, or life imprisonment if the crime results in death. See 18 U.S.C. § 1993.

Harboring Terrorists - Previously the harboring offense prohibited only the harboring of spies (see 18 U.S.C. §792); there was no comparable terrorism provision. The new

law prohibits harboring or concealing persons who have committed or are about to commit a variety of terrorist offenses, including destruction of aircraft or aircraft facilities, use of nuclear materials or chemical or biological weapons, use of weapons of mass destruction, arson or bombing of government property, destruction of energy facilities, sabotage of nuclear facilities, or aircraft piracy. See 18 U.S.C. § 2339.

Expert Advice/Assistance and Material Support - The prohibition on providing material support or resources to terrorists was expanded to include expert advice and assistance. This makes the offense applicable to experts who provide advice or assistance knowing or intending that it is to be used in preparing for or carrying out terrorism crimes, such as the civil engineer providing advice on the best manner to destroy a building. This provision expanded the criminal law by eliminating the restriction that such material support be within the United States, clarifying that prohibited material support includes all types of monetary instruments, and adding to the list of underlying terrorism crimes for which provision of material support is barred. Additionally, material support offenses can be prosecuted in any district in which the underlying offense was committed. The Act also clarified that the Trade Sanctions Reform and Export Enhancement Act of 2000 does not limit this prohibition. See 18 U.S.C.§ 2339A.

Possession of a Biological Agent - The Act established an additional offense to the biological weapons statute of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose. Additionally it created a new offense for certain restricted persons (including felons, persons indicted for felonies, fugitives, drug users, illegal aliens, mentally impaired persons, aliens from certain terrorist states, and persons dishonorably discharged from the U.S. armed services) to possess a biological agent or toxin listed as a "select agent" by the Secretary of Health and Human Services. See 18 U.S.C. § 175.

Attempt and Conspiracy - The Act amended several terrorism crimes to add a prohibition on attempt and conspiracy resulting in penalties equal to the underlying offenses. See 18 U.S.C. § 81 (arson); 18 U.S.C. § 930(c) (killings in federal facilities); 18 U.S.C. § 1362 (injuring or destroying communications lines or systems); 18 U.S.C. § 1363 (injuring or destroying buildings or property within the special maritime and territorial jurisdiction of the United States); 18 U.S.C. § 1992 (wrecking trains); 18 U.S.C. § 2339A (material support to terrorists); 18 U.S.C. § 2340A (torture); 42 U.S.C. § 2284 (sabotage of nuclear facilities or fuel); 49 U.S.C. § 46504 (interference with flight crew members and attendants); 49 U.S.C. § 46505 (carrying weapons aboard aircraft); and 49 U.S.C. § 60123(b) (damaging or destroying an interstate gas or hazardous liquid pipeline facility).

Additional Information and Manual Changes

Additional guidance and associated manual changes will be forthcoming. Any questions should be directed to the Investigative Law Unit, [redacted] The text of the law,

b2

redline/strikeout text of affected statutes and Federal Rules, and other associated documents are posted on [redacted] which can be found through [redacted]

LEAD (s): b2

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to all appropriate personnel.

CC: Mr. Parkinson, Rm 7427
Mr. Steele, Rm. 7159
Mr. Kelley, Rm. 7427
Ms. Gulyassy, Rm. 7159
Ms. Lammert, Rm. 7326
[redacted] Rm. 7879
[redacted] Rm. 7975 b6
[redacted] Rm. 7975 b7C
[redacted] Rm. 7879
[redacted] Rm. 7877
ILU
Each OGC Unit Chief

♦♦

Order Code RL30465

CRS Report for Congress
Received through the CRS Web

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions

Updated September 22, 2004

Elizabeth B. Bazan
Legislative Attorney
American Law Division

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions

Summary

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, (FISA) as passed in 1978, provided a statutory framework for the use of electronic surveillance in the context of foreign intelligence gathering. In so doing, the Congress sought to strike a delicate balance between national security interests and personal privacy rights. Subsequent legislation expanded federal laws dealing with foreign intelligence gathering to address physical searches, pen registers and trap and trace devices, and access to certain business records. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56, made significant changes to some of these provisions. Further amendments were included in the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, and the Homeland Security Act of 2002, P.L. 107-296. In addressing international terrorism or espionage, the same factual situation may be the focus of both criminal investigations and foreign intelligence collection efforts. The changes in FISA under these public laws facilitate information sharing between law enforcement and intelligence elements. In its Final Report, the 9/11 Commission noted that the removal of the pre-9/11 "wall" between intelligence and law enforcement "has opened up new opportunities for cooperative action within the FBI."

On May 17, 2002, the U.S. Foreign Intelligence Surveillance Court (FISC) issued a memorandum opinion and order written by the then Presiding Judge of the court, and concurred in by all of the other judges then on the court. The unclassified opinion and order were provided to the Senate Judiciary Committee in response to a letter from Senator Leahy, Senator Grassley, and Senator Specter, who released them to the public on August 22, 2002. In the decision, the FISC considered a motion by the U.S. Department of Justice "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion." The FISC granted the Department's motion, but modified part of the proposed minimization procedures. While this FISC decision was not appealed directly, the Department of Justice did seek review of an FISC order authorizing electronic surveillance of an agent of a foreign power and of an FISC order renewing that surveillance, both subject to restrictions based upon the May 17th memorandum opinion and order by the FISC. The U.S. Foreign Intelligence Surveillance Court of Review reversed and remanded the FISC orders on November 18, 2002.

This report will examine the detailed statutory structure provided by FISA and related provisions of E.O. 12333. In addition, it will discuss the decisions of the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review. Bills from the 108th Congress relating to FISA are addressed in CRS Report RL32608, *Foreign Intelligence Surveillance Act: Selected Legislation from the 108th Congress.*

Contents

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions

Introduction

On October 26, 2001, President George W. Bush signed P.L. 107-56, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act or the USA PATRIOT Act. Among its provisions are a number which impacted or amended the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* (FISA). For example, the new law expanded the number of United States district court judges on the Foreign Intelligence Surveillance Court and provided for roving or multipoint electronic surveillance authority under FISA. It also amended FISA provisions with respect to pen registers and trap and trace devices and access to business records. In addition, FISA, as amended, substantially expanded the reach of the business records provisions. The amended language changed the certification demanded of a federal officer applying for a FISA order for electronic surveillance from requiring a certification that *the* purpose of the surveillance is to obtain foreign intelligence information to requiring certification that *a significant purpose* of the surveillance is to obtain foreign intelligence information. FISA, as amended, also affords persons aggrieved by inappropriate use or disclosure of information gathered in or derived from a FISA surveillance, physical search or use of a pen register or trap and trace device a private right of action. Of the amendments made by the USA PATRIOT Act, all but the section which increased the number of judges on the Foreign Intelligence Surveillance Court will sunset on December 31, 2005. Subsequent amendments to FISA were made by the Intelligence Authorization Act for Fiscal Year 2003, P.L. 107-108 (H.R. 2883), and by the Homeland Security Act of 2002, P.L. 107-296.

On May 17, 2002, the U.S. Foreign Intelligence Surveillance Court (FISC) issued an opinion and order[1] written by the then Presiding Judge of the court, U.S. District Judge Royce C. Lamberth. All of the other judges then on the FISC concurred in the order. The opinion was provided by the current Presiding Judge of the FISC, U.S. District Judge Colleen Kollar-Kotelly, to the Senate Judiciary Committee in response to a July 31 letter from Senator Leahy, Senator Grassley and

---

[1] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611(U.S. Foreign Intell. Surveil. Ct. 2002) (hereinafter *FISC op.*).

Senator Specter.[2] On August 22, 2002, the unclassified opinion was released to the public by Senator Leahy, Senator Grassley and Senator Specter.

In the memorandum opinion and order, the FISC considered a motion by the U.S. Department of Justice "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion."[3] In its memorandum and accompanying order, the FISC granted the Department of Justice's motion, but modified the second and third paragraphs of section II.B of the proposed minimization procedures.[4]

The FISC's May 17th memorandum opinion and order were not appealed directly. However, the Justice Department sought review in the U.S. Foreign Intelligence Court of Review (Court of Review) of an FISC order authorizing electronic surveillance of an agent of a foreign power, subject to restrictions flowing from the May 17th decision, and of an FISC order renewing that surveillance subject to the same restrictions.[5] The Court of Review reversed and remanded the FISC orders.[6] This opinion, the first issued by the U.S. Foreign Intelligence Surveillance

---

[2] *See,* Statement of Sen. Patrick Leahy, Chairman, Committee on the Judiciary, "The USA PATRIOT Act in Practice: Shedding Light on the FISA Process" (Sept. 10, 2002), [http://leahy.senate.gov/press/2002209/091002.html]; "Courts," *National Journal's Technology Daily* (August 22, 2002, PM Edition); "Secret Court Rebuffs Ashcroft; Justice Dept. Chided on Misinformation," by Dan Eggen and Susan Schmidt, *Washington Post*, p. A1 (August 23, 2002).

[3] *FISC op.*, 218 F. Supp. 2d at 613.

[4] *Id.* at 624-27.

[5] In re Sealed Case, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002) (hereinafter *Court of Review op.*).

[6] The Foreign Intelligence Surveillance Act, P.L. 95-511, as amended (hereinafter FISA), Title I, § 103, 50 U.S.C. § 1803, created both the U.S. Foreign Intelligence Surveillance Court and the U.S. Foreign Intelligence Surveillance Court of Review. As originally constituted the FISC was made up of 7 U.S. district court judges publicly designated by the Chief Justice of the United States. As amended by the USA PATRIOT Act, P.L. 107-56, § 208, the membership in the FISC was expanded to 11 members, at least 3 of whom must live within a 20 mile radius of the District of Columbia. The U.S. Foreign Intelligence Surveillance Court of Review is made up of 3 U.S. district court or U.S. court of appeals judges publicly designated by the Chief Justice.

The current language of 50 U.S.C. § 1803 provides:

§ 1803. Designation of judges

(a) Court to hear applications and grant orders; record of denial; transmittal to court of review

The Chief Justice of the United States shall publicly designate 11 district court judges from seven of the United States judicial circuits of whom no fewer

(continued...)

[6] (...continued)

than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established under subsection (b) of this section.

(b) Court of review; record, transmittal to Supreme Court

The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

(c) Expeditious conduct of proceedings; security measures for maintenance of records

Proceedings under this chapter shall be conducted as expeditiously as possible. The record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence.

(d) Tenure

Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) of this section shall be designated for terms from one to seven years so that one term expires each year, and that judges first designated under subsection (b) of this section shall be designated for terms of three, five, and seven years.

The reference in subsection (a), (b), and (c) to "this chapter" refers to chapter 36 of Title 18, U.S.C., where the Foreign Intelligence Surveillance Act, as amended, is codified. This act, as amended, deals with electronic surveillance (50 U.S.C. § 1801 *et seq.*), physical searches (50 U.S.C. § 1821 *et seq.*), pen registers and trap and trace devices (50 U.S.C. § 1841 *et seq.*), and "access to certain business records for foreign intelligence and international terrorism investigations" (50 U.S.C. § 1861). The judges of the FISC are given jurisdiction over applications for physical searches for the purpose of obtaining foreign intelligence information anywhere in the United States under 50 U.S.C. § 1822(c). Under 50 U.S.C. § 1842(b), an application for an order authorizing or approving the installation and use of a

(continued...)

Court of Review since its creation in 1978, was also released to the public. This report will provide background on the Foreign Intelligence Surveillance Act, discuss its statutory framework, and review these two decisions.

Background

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests.[7] The stage was set for legislation to address these competing concerns in part by Supreme Court decisions on related issues. In *Katz v. United States*, 389 U.S. 347 (1967), the Court held that the protections of the Fourth Amendment extended to circumstances involving electronic surveillance of oral communications without physical intrusion.[8] The *Katz* Court stated, however, that its holding did not extend to cases involving national security.[9] In *United States v. United States District Court*, 407 U.S. 297 (1972) (the *Keith* case), the Court regarded *Katz* as "implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[10] Mr. Justice Powell, writing for the *Keith* Court, framed the matter before the Court as follows:

> The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right

---

[6] (...continued)
pen register or trap and trace device for foreign intelligence or international terrorism investigations may be made to either a judge of the FISC or to a U.S. Magistrate Judge publicly designated by the Chief Justice of the United States to have the power to hear applications for and grant orders on behalf of an FISC judge approving such installation and use. Similarly, under 50 U.S.C. § 1861(b), an application for an order for production of tangible things under the "business records" provision may be made either to an FISC judge or to a U.S. Magistrate Judge publicly designated by the Chief Justice of the United States to hear such an application and to grant such an order on behalf of an FISC judge.

[7] The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[8] Katz v. United States, 389 U.S. 347, 353 (1967).

[9] *Id.*, at 359, n. 23.

[10] United States v. United States District Court, 407 U.S. 297, 313-14 (1972).

> to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.[11]

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.[12] Justice Powell emphasized that the case before it "require[d] no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country."[13] The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents."[14] However, the guidance which the Court provided in *Keith* with respect to national security surveillance in a domestic context to some degree presaged the approach Congress was to take in foreign intelligence surveillance. The *Keith* Court observed in part:

> . . . We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crimes. Given these potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. . . . It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not

---

[11] 407 U.S. at 299.

[12] *Id.*, at 391-321. Justice Powell also observed that,

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961). . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." . . . .

[13] *Id.*, at 308.

[14] *Id.*, at 321-22.

> follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . .; and that the time and reporting requirements need not be so strict as those in § 2518. The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.[15]

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of Brown, an American citizen, was incidentally overheard. The Third Circuit in *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom, Ivanov v. United States*, 419 U.S. 881 (1974), concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information. In its plurality decision in *Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976), the District of Columbia Circuit took a somewhat different view in a case involving a warrantless wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power. Finding that a warrant was required in such circumstances, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."

With the passage of the Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified as amended at 50 U.S.C. § 1801 *et seq.*, Congress sought to strike a delicate balance between these interests when the gathering of foreign intelligence involved the use of electronic surveillance.[16] Collection of foreign intelligence information through electronic surveillance is now governed by FISA and E.O. 12333.[17] This report will examine the provisions of

---

[15] 407 U.S. at 323-24.

[16] For an examination of the legislative history of P.L. 95-511, see S. Rept. 95-604, Senate Committee on the Judiciary, Parts I and II (Nov. 15, 22, 1977); S. Rept. 95-701, Senate Select Committee on Intelligence (March 14, 1978); H.Rept. 95-1283, House Permanent Select Committee on Intelligence (June 8, 1978); H. Conf. Rept. 95-1720 (Oct. 5, 1978); Senate Reports and House Conference Report are reprinted in 1978 *U.S. Code Cong. & Admin. News* 3904.

[17] Physical searches for foreign intelligence information are governed by 50 U.S.C. § 1821 *et seq.*, while the use of pen registers and trap and trace devices in connection with foreign intelligence investigations is addressed in 50 U.S.C. § 1841 *et seq.* Access to certain (continued...)

FISA which deal with electronic surveillance, in the foreign intelligence context, as well as those applicable to physical searches, the use of pen registers and trap and trace devices under FISA, and access to business records and other tangible things for foreign intelligence purposes. As the provisions of E.O. 12333 to some extent set the broader context within which FISA operates, we will briefly examine its pertinent provisions first.

Executive Order 12333

Under Part 2.3 of E.O. 12333, the agencies within the Intelligence Community are to "collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. . . ." Among the types of information that can be collected, retained or disseminated under this section are:

> (a) Information that is publicly available or collected with the consent of the person concerned;
>
> (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
>
> (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;
>
> (d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;
>
> (e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting;
>
> (f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
>
> (g) Information arising out of a lawful personnel, physical or communications security investigation;
>
> . . .
>
> (i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and
>
> (j) Information necessary for administrative purposes.

---

[17] (...continued)
business records for foreign intelligence or international terrorism investigative purposes is covered by 50 U.S.C. § 1861 *et seq.*

> In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

In discussing collections techniques, Part 2.4 of E.O. 12333 indicates that agencies within the Intelligence Community are to use

> the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. . . .

Part 2.5 of the Executive Order 12333 states that:

> The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978 [section 1801 et seq. of this title], shall be conducted in accordance with that Act, as well as this Order.

The Foreign Intelligence Surveillance Act

The Statutory Framework

Electronic surveillance under FISA. The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, as amended, provides a framework for the use of electronic surveillance,[18] physical searches, pen registers and trap and trace devices

---

[18] 50 U.S.C. § 1801(f)(2) defines "electronic surveillance" to mean:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any person thereto, if such acquisition occurs in the United States, *but does not include the acquisition of those communications of*

(continued...)

to acquire foreign intelligence information.[19] This measure seeks to strike a balance

---

[18] (...continued)

computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

The italicized portion of Subsection 1801(f)(2) was added by Sec. 1003 of P.L. 107-56.

[19] "Foreign intelligence information" is defined in 50 U.S.C. § 1801(e) to mean:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power;

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

"International terrorism" is defined in 50 U.S.C. § 1801(c) to mean activities that:

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended–

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

"Sabotage" is defined in 50 U.S.C. § 1801(d) to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."

between national security needs in the context of foreign intelligence gathering and privacy rights.[20]

Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance to acquire foreign intelligence information for up to one year without a court order if two criteria are satisfied. First, to utilize this authority, the Attorney General must certify in writing under oath that:

> (A) the electronic surveillance is solely directed at —
>
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
>
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2) or (3) of this title;
>
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

---

[20] In addition to the provisions dealing with electronic surveillance, physical searches and pen registers and trap and trace devices, FISA includes a section which permits the Director of the FBI or his designee (whose rank may be no lower than an Assistant Special Agent in Charge) to apply for an order requiring "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities . . . ." 50 U.S.C. § 1861(a)(1). Where such an investigation is of a United States person, it may not be conducted "solely upon the basis of activities protected by the first amendment to the Constitution." *Id.* Although this section is entitled "access to certain business records for foreign intelligence and international terrorism investigations," it encompasses substantially more than just business records. The current language of 50 U.S.C. §§ 1861 and 1862 (which deals with congressional oversight of all such requests for production of tangible things under § 1861) was added by the USA PATRIOT Act, and amended by P.L. 107-108. It replaced former 50 U.S.C. §§ 1861-1863, added by P.L. 105-272, title VI, § 602, 112 Stat. 2411 (Oct. 20, 1998), which defined various terms, provided for applications for orders for access to certain limited types of business records (relating to records in the possession of common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities) for foreign intelligence and international terrorism investigations, and provided for congressional oversight of such records requests.

H.R. 1157, 108th Congress, as introduced, would amend 50 U.S.C. § 1861 to prohibit applications from being made under that section "with either the purpose or effect of searching for, or seizing from, a bookseller or library documentary materials that contain personally identifiable information concerning a patron of a bookseller or library," but would not preclude a physical search for such documentary materials under other provisions of law. This measure would also expand reporting requirements with respect to applications for tangible things under 50 U.S.C. § 1861. H.R. 1157 was introduced March 6, 2003 and referred to the House Judiciary Committee and the House Permanent Select Committee on Intelligence. On May 5, 2003, it was referred to the Subcommittee on Crime, Terrorism, and Homeland Security of the House Judiciary Committee.

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title;[21] . . . .

---

[21] Minimization procedures with respect to electronic surveillance are defined in 50 U.S.C. § 1801(h) to mean:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
>
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than *72* hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Sec. 314(a)(1) of H.Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002 to accompany H.R. 2883, amended 50 U.S.C. § 1801(h)(4) to change to 72 hours what was previously a 24 hour period beyond which the contents of any communication to which a U.S. person is a party may not be retained absent a court order under 50 U.S.C. § 1805 or a finding by the Attorney General that the information indicates a threat of death or serious bodily injury. The conference version of H.R. 2883 received the approbation of both houses of Congress, and was forwarded to the President on December 18, 2001, for his signature. It became P.L. 107-108.

"United States person" is defined in 50 U.S.C. § 1801(i) to mean

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

"Foreign power" is defined in 50 U.S.C. § 1801(a) to mean:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;

(continued...)

[21] (...continued)

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

"Agent of a foreign power" is defined in 50 U.S.C. § 1801(b) to mean:

(1) any person other than a United States person, who--

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who--

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

As introduced, both S. 113 and a parallel bill S. 123, 108th Congress, would amend the definition of "foreign power" in 50 U.S.C. § 1801(a)(4) to read "a person, other than a United States person, or a group that is engaged in international terrorism or activities in preparation therefor." As reported out of the Senate Judiciary Committee on March 11, 2003, S. 113, 108th Congress, would strike this language amending the definition of "foreign power" in 50 U.S.C. § 1801(a)(4), and would instead amend the definition of "agent of a

(continued...)

Second, in order for the President, through the Attorney General, to use this authority

> . . . the Attorney General [must report] such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization and the reason for their becoming effective immediately.

Such electronic surveillance must be conducted only in accordance with the Attorney General's certification and minimization procedures adopted by him. A copy of his certification must be transmitted by the Attorney General to the court established under 50 U.S.C. § 1803(a) (hereinafter the FISC).[22] This certification remains under

---

[21] (...continued)
foreign power" in 50 U.S.C. § 1801(b)(1) to add a new subparagraph "(C) engages in international terrorism or activities in preparation therefor; or." The effect of this language would be to included in the definition of "agent of a foreign power" non-U.S. persons who engage in international terrorism without requiring affiliation with an international terrorist group. During floor consideration, S. 113 as reported was amended to permit a court, upon application by the Federal official seeking a FISA order, to presume that a non-U.S. person who is knowingly engaged in sabotage or international terrorism, or activities that are in preparation therefore, is an agent of a foreign power. This provision would be "subject to the sunset provision in section 224 of the USA PATRIOT Act of 2001 (Public Law 107-56, 115 Stat. 295), including the exception provided in subsection (b) of such section 224." The sunset provision in Section 224 of P.L. 107-56, would take effect on December 31, 2005. S. 113 passed the Senate on May 8, 2003. The measure was referred to the House Subcommittee on Crime, Terrorism and Homeland Security on June 25, 2003. A precursor of S. 113 and S. 123, as introduced, was S. 2586, introduced in the 107th Congress. Hearings were held on that measure before the Senate Select Committee on Intelligence on July 31, 2002. S. 123 was referred to the Senate Judiciary Committee on January 9, 2003. For a more detailed discussion of S. 113, see CRS Report RS21472, by Jennifer Elsea, entitled "Proposed Change to the Foreign Intelligence Surveillance Act (FISA) under S. 113" (August 9, 2004).

Section 1503 of S. 22, 108th Congress, if enacted, would, in effect, eliminate the sunset provision (as applicable to all sections not excepted from its terms by Section 224), by bringing all of those provisions which would sunset on December 31, 2005, back into force on January 1, 2006. S. 22 was referred to the Senate Judiciary Committee on January 7, 2003.

[22] Under 50 U.S.C. § 1803(a), as amended by Section 208 of P.L. 107-56, the Chief Justice of the United States must publicly designate eleven U.S. district court judges from seven of the United States judicial circuits, of whom no fewer than three must reside within 20 miles of the District of Columbia. These eleven judges constitute the court which has jurisdiction over applications for and orders approving electronic surveillance anywhere within the United States under FISA. If an application for electronic surveillance under this act is denied by one judge of this court, it may not then be considered by another judge on the court. If a judge denies such an application, he or she must immediately provide a written statement for the record of the reason(s) for this decision. If the United States so moves, this
(continued...)

[22] (...continued)
record must then be transmitted under seal to a court of review established under 50 U.S.C. § 1803(b). The Chief Justice also publicly designates the three U.S. district court or U.S. court of appeals judges who together make up the court of review having jurisdiction to review any denial of an order under FISA. If that court determines that an application was properly denied, again a written record of the reason(s) for the court of review's decision must be provided for the record, and the United States may petition for a writ of certiorari to the United States Supreme Court. All proceedings under this act must be conducted expeditiously, and the record of all proceedings including applications and orders granted, must be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence. 50 U.S.C. § 1803(c).

Section 2 of S. 436, 108th Congress, as introduced, would add a new 50 U.S.C. §1803(e), authorizing the FISC and the Foreign Intelligence Surveillance Court of Review "to establish such rules and procedures, and take such actions, as are reasonably necessary to administer their responsibilities under this act." These rules and procedures would be recorded and transmitted to the judges of these two courts, the Chief Justice of the United States, the House and Senate Judiciary Committees, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence. S. 436 also includes new reporting requirements. The Attorney General would be required to issue a public annual report on: aggregate numbers of U.S. persons targeted for orders issued under FISA for electronic surveillance, physical searches, pen registers, and access to records under section 501 of the act (18 U.S.C. § 1861); the number of times the Attorney General has authorized information obtained under 50 U.S.C. §§ 1806, 1824, 1842, or 1861, or any derivative information, to be used in a criminal proceedings; and the number of times that a statement which is required under 50 U.S.C. §§ 1806(b) (electronic surveillance), 1825(c) (physical searches), or 1845(b) (pen registers) to accompany disclosure of information obtained under FISA or derived therefrom was completed, stating that such information "may only be used in a criminal proceeding with the advance authorization of the Attorney General." In addition, S. 436 would require the Attorney General's public report to include, "in a manner consistent with the protection of the national security of the United States,":

> (A) the portions of the documents and applications filed with the courts established under section 103 [50 U.S.C. § 1803] that include significant construction or interpretation of the provisions of this Act or any provision of the United States Constitution, not including the facts of any particular matter, which may be redacted;
> (B) the portions of the opinions of the orders of the courts established under section 103 that include significant construction or interpretation of the provisions of this Act or any provision of the United States Constitution, not including the facts of any particular matter, which may be redacted; and
> (C) in the first report submitted under this section, the matters specified in subparagraphs (A) and (B) for all documents and applications filed with the courts established under section 103, and all otherwise unpublished opinions and orders of that court, for the 4 years before the preceding calendar year in addition to that year.".

Section 3 of S. 436 would also add a new sentence to 18 U.S.C. § 2709(e), dealing with counterintelligence access to telephone toll and transactional records. Subsection 2709(e) requires the Director of the FBI, on a semiannual basis, to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, the Senate Judiciary Committee and the House Judiciary Committee,
(continued...)

seal unless an application for a court order for surveillance authority is made under 50 U.S.C. §§ 1801(h)(4) and 1804,[23] or the certification is necessary to determine the legality of the surveillance under 50 U.S.C. § 1806(f).[24] 50 U.S.C. § 1802(a)(2) and (a)(3).

In connection with electronic surveillance so authorized, the Attorney General may direct a specified communications common carrier to furnish all information, facilities, or technical assistance needed for the electronic surveillance to be accomplished in a way that would protect its secrecy and minimize interference with the services provided by the carrier to its customers. 50 U.S.C. § 1802(a)(4)(A). In addition, the Attorney General may direct the specified communications common carrier to maintain any records, under security procedures approved by the Attorney General and the Director of Central Intelligence, concerning the surveillance or the assistance provided which the carrier wishes to retain. 50 U.S.C. § 1802(a)(4)(B). Compensation at the prevailing rate must be made to the carrier by the Government for providing such aid.

If the President, by written authorization, empowers the Attorney General to approve applications to the FISC, an application for a court order may be made pursuant to 50 U.S.C. § 1802(b). A judge receiving such an application may grant an order under 50 U.S.C. § 1805 approving electronic surveillance of a foreign power or an agent of a foreign power to obtain foreign intelligence information. There is an exception to this, however. Under 50 U.S.C. § 1802(b), a court does not have jurisdiction to grant an order approving electronic surveillance directed solely as described in 50 U.S.C. § 1802(a)(1)(A) (that is, at acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, or acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power), unless the surveillance may involve the acquisition of communications of a United States person. 50 U.S.C. § 1802(b).

An application for a court order authorizing electronic surveillance for foreign intelligence purposes may be sought under 50 U.S.C. § 1804. An application for such a court order must be made by a federal officer in writing on oath or affirmation to an FISC judge. The application must be approved by the Attorney General based upon his finding that the criteria and requirements set forth in 50 U.S.C. § 1801 *et seq.* have been met. Section 1804(a) sets out what must be included in the application:

(1) the identity of the Federal officer making the application;

---

[22] (...continued)
concerning all requests made under subsection 2709(b). Section 3 of S. 436, as introduced, would require that the information provided under 18 U.S.C. § 2709(e) "shall include a separate statement of all such requests made of institutions operating as public libraries or serving as libraries of secondary schools or institutions of higher education." S. 436 was referred to the Senate Judiciary Committee on February 25, 2003.

[23] 50 U.S.C. § 1804 is discussed at pages 15-20 of this report, *infra.*

[24] 50 U.S.C. § 1806 is discussed at pages 27-33 of this report, *infra.*

(2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;

(3) the identity, if known, or a description of the target of the electronic surveillance;

(4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that —

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(5) a statement of the proposed minimization procedures;

(6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate[25]—

(A) that the certifying official deems the information sought to be foreign intelligence information;

---

[25] Under Section 1-103 of Executive Order 12139, the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the FBI, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence were designated to make such certifications in support of applications to engage in electronic surveillance for foreign intelligence purposes. Neither these officials nor anyone acting in those capacities may make such certifications unless they are appointed by the President with the advice and consent of the Senate.

(B) that *a significant*[26] purpose of the surveillance is to obtain foreign

---

[26] Section 218 of P.L. 107-56 amended the requisite certifications to be made by the Assistant to the President for National Security Affairs, or other designated official (see footnote 18). Heretofore, the certifying official had to certify, among other things, that *the* purpose of the electronic surveillance under FISA was to obtain foreign intelligence information. Under the new language, the certifying official must certify that *a significant* purpose of such electronic surveillance is to obtain foreign intelligence information. This change may have the effect of somewhat blurring the line between electronic surveillance for foreign intelligence purposes and that engaged in for criminal law enforcement purposes.

Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, United States v. Megahey, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), *aff'd* 729 F.2d 1444 (2d Cir. 1982); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987); United States. v Badia, 827 F. 2d 1458, 1464 (11th Cir. 1987). *See also*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), *rehearing and cert. denied*, 506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); United States v. Pelton, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S.1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard–i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense--for issuance of a search warrant was violative of the 4th Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); United States v. Rahman, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). *Cf.*, United States v. Bin Laden, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); United States v. Bin Laden, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection. . . . If foreign intelligence collection is merely *a* purpose and not the *primary* purpose of a search, the exception does not apply.") *Cf.*, United States v. Sarkissian, 841 F.2d 959, 964-65 (9th Cir. 1988) (FISA court order authorizing electronic surveillance, which resulted in the discovery of plan to bomb the Honorary Turkish Consulate in Philadelphia, and of the fact that bomb components were being transported by plane from Los Angeles. The FBI identified the likely airlines, flight plans, anticipated time of arrival, and suspected courier. Shortly before the arrival of one of those flights, the investigation focused upon an individual anticipated to be a passenger on a particular flight meeting all of the previously identified criteria. An undercover police officer spotted a man matching the suspected courier's description on that flight. The luggage from that flight was sniffed by a trained dog and x-rayed. A warrantless search was conducted of a suitcase that had been shown by

(continued...)

[26] (...continued)
x-ray to contain an unassembled bomb. Defendants unsuccessfully moved to suppress the evidence from the FISA wiretap and the warrantless search. On appeal the court upheld the warrantless suitcase search as supported by exigent circumstances. Defendants contended that the FBI's primary purpose for the surveillance had shifted at the time of the wiretap from an intelligence investigation to a criminal investigation and that court approval for the wiretap therefore should have been sought under Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*, rather than FISA. The court, while noting that in other cases it had stated that "the purpose of [electronic] surveillance" under FISA "must be to secure foreign intelligence information", "not to ferret out criminal activity," declined to decide the issue of whether the standard under FISA required "the purpose" or "the primary purpose" of the surveillance to be gathering of foreign intelligence information. The court stated, "Regardless of whether the test is one of purpose or primary purpose, our review of the government's FISA materials convinces us that it is met in this case. . . . We refuse to draw too fine a distinction between criminal and intelligence investigations. "International terrorism ," by definition, requires the investigation of activities that constitute crimes. 50 U.S.C. § 1806(f). That the government may later choose to prosecute is irrelevant. FISA contemplates prosecution based on evidence gathered through surveillance. . . . "Surveillances . . . need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate." S. Rep. No. 701, 95th Cong., 1st Sess. 11 . . . .[(1978)]. . . .FISA is meant to take into account "the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities . . ." *Id.* . . . . At no point was this case an ordinary criminal investigation."). *Cf.,* United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) (distinguishing United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980); and United States v. Butenko, 494 F.2d 593, 606 (3d Cir.) (*en banc*), *cert. denied sub nom,* Ivanov v. United States, 419 U.S. 881 (1974), which held that, while warrantless electronic surveillance for foreign intelligence purposes was permissible, when the purpose or primary purpose of the surveillance is to obtain evidence of criminal activity, evidence obtained by warrantless electronic surveillance is inadmissible at trial, 540 F. Supp. at 1313; on the theory that the evidence in the case before it was obtained pursuant to a warrant–a lawfully obtained court order under FISA, *id.* at 1314. The court noted that the "bottom line of *Truong* is that evidence derived from *warrantless* foreign intelligence searches will be admissible in a criminal proceeding only so long as the primary purpose of the surveillance is to obtain foreign intelligence information." *Id.* at 1313-14. After noting that Congress, in enacting FISA, "expected that evidence derived from FISA surveillances could then be used in a criminal proceeding," the court concluded that "it was proper for the FISA judge to issue the order in this case because of the on-going nature of the foreign intelligence investigation. . . . The fact that evidence of criminal activity was thereafter uncovered during the investigation does not render the evidence inadmissible. There is no question in [the court's] mind that the purpose of the surveillance, pursuant to the order, was the acquisition of foreign intelligence information. Accordingly, [the court found] that the FISA procedures on their face satisfy the Fourth Amendment warrant requirement, and that FISA was properly implemented in this case." *Id.* at 1314.).

It is worthy of note that none of these decisions were handed down by the U.S. Foreign Intelligence Surveillance Court or the U.S. Foreign Intelligence Surveillance Court of Review. For a discussion of the recent decisions of those two courts regarding the Attorney General's 2002 minimization procedures, please see the discussion in the portion of this report regarding "Recent Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review," *infra.* Nor do the decisions of the U.S. district courts and
(continued...)

intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in 1801(e) of this title; and

(E) including a statement of the basis for the certification that —

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more that one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

The application for a court order need not contain the information required in Subsections 1804(6), (7)(E), (8), and (11) above if the target of the electronic surveillance is a foreign power and each of the facilities or places at which surveillance is directed is owned, leased, or exclusively used by that foreign power. However, in those circumstances, the application must indicate whether physical entry is needed to effect the surveillance, and must also contain such information about the surveillance techniques and communications or other information regarding United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures. 50 U.S.C. § 1804(b).

---

[26] (...continued)
U.S. courts of appeal reflect recent legislative amendments to the FISA statute. However, the FISC, in its decision, did not address potential Fourth Amendment implications, and the U.S. Foreign Intelligence Court of Review, in its decision, appears to imply that some Fourth Amendment issues in the FISA context may be non-justiciable. Alternatively, the language in the Court of Review opinion might mean that the issue has not yet been considered by the courts. Using a balancing test it derived from *Keith* between foreign intelligence crimes and ordinary crimes, the Court of Review found surveillances under FISA, as amended by the USA PATRIOT Act, to be reasonable and therefore constitutional, while at the same time acknowledging that the constitutional question presented by the case before it–"whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment–has no definitive jurisprudential answer." *Court of Review op.*, 301 F.3d at 746.

Where an application for electronic surveillance under 50 U.S.C. § 1804(a) involves a target described in 50 U.S.C. § 1801(b)(2),[27] the Attorney General must personally review the application if requested to do so, in writing, by the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of Central Intelligence.[28] The authority to make such a request may not be delegated unless the official involved is disabled or otherwise unavailable.[29] Each such official must make appropriate arrangements, in advance, to ensure that such a delegation of authority is clearly established in case of disability or other unavailability.[30] If the Attorney General determines that an application should not be approved, he must give the official requesting the Attorney General's personal review of the application written notice of the determination. Except in cases where the Attorney General is disabled or otherwise unavailable, the responsibility for such a determination may not be delegated. The Attorney General must make advance plans to ensure that the delegation of such responsibility where the Attorney General is disabled or otherwise unavailable is clearly established.[31] Notice of the Attorney General's determination that an application should not be approved must indicate what modifications, if any, should be made in the application needed to make it meet with the Attorney General's approval.[32] The official receiving the Attorney General's notice of modifications which would make the application acceptable must modify the application if the official deems such modifications warranted. Except in cases of disability or other unavailability, the responsibility to supervise any such modifications is also a non-delegable responsibility.[33]

If a judge makes the findings required under 50 U.S.C. § 1805(a), then he or she must enter an ex parte order as requested or as modified approving the electronic surveillance. The necessary findings must include that:

> (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
>
> (2) the application has been made by a Federal officer and approved by the Attorney General;
>
> (3) on the basis of the facts submitted by the applicant there is probable cause to believe that —
>
> > (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

---

[27] For a list of those covered in 50 U.S.C. § 1801(b)(2), see footnote 14, *supra*.

[28] 50 U.S.C. § 1804(e)(1)(A).

[29] 50 U.S.C. § 1804(e)(1)(B).

[30] 50 U.S.C. § 1804(e)(1)(C).

[31] 50 U.S.C. § 1804(e)(2)(A).

[32] 50 U.S.C. § 1804(e)(2)(B).

[33] 50 U.S.C. § 1804(e)(2)(C).

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

In making a probable cause determination under 50 U.S.C. § 1805(a)(3), the judge may consider past activities of the target as well as facts and circumstances relating to the target's current or future activities.[34] An order approving an electronic surveillance under Section 1805(c) must:

(1) specify–

(A) the identity, if known, or a description of the target of the electronic surveillance;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, *if known*;[35]

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the device involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct–

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant a specified communication or other common carrier, landlord, custodian, or other specified person, *or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,* furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

---

[34] 50 U.S.C. § 1805(b).

[35] Section 314(a)(2)(A) of H.Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002, to accompany H.R. 2883, added "if known" to the end of Section 1805(c)(1)(B) before the semi-colon. The conference version of the bill passed both the House and the Senate, and was signed by the President on December 28, 2001.

> (D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.[36]

The italicized portions of Section 1805(c)(1)(B) and Section1805(c)(2)(B) reflect changes, added by P.L. 107-108 and P.L. 107-56 respectively, intended to provide authority for "multipoint" or "roving" electronic surveillance where the actions of the target of the surveillance, such as switching phones and locations repeatedly, may thwart that surveillance. The Conference Report on H.R. 2338, the Intelligence Authorization Act for Fiscal Year 2002, H.Rept. 107-328, at page 24, provided the following explanation of these changes:

> The multipoint wiretap amendment to FISA in the USA PATRIOT Act (section 206) allows the FISA court to issue generic orders of assistance to any communications provider or similar person, instead of to a particular communications provider. This change permits the Government to implement new surveillance immediately if the FISA target changes providers in an effort to thwart surveillance. The amendment was directed at persons who, for example, attempt to defeat surveillance by changing wireless telephone providers or using pay phones.
>
> Currently, FISA requires the court to "specify" the "nature and location of each of the facilities or places at which the electronic surveillance will be directed." 50 U.S.C. § 105(c)(1)(B). Obviously, in certain situations under current law, such a specification is limited. For example, a wireless phone has no fixed location and electronic mail may be accessed from any number of locations.
>
> To avoid any ambiguity and clarify Congress' intent, the conferees agreed to a provision which adds the phrase, "if known," to the end of 50 U.S.C. § 1805(c)(1)(B). The "if known" language, which follows the model of 50 U.S.C. § 1805(c)(1)(A), is designed to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.

If the target of the electronic surveillance is a foreign power and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order does not need to include the information covered by Section 1805(c)(1)(C), (D), and (F), but must generally describe the information sought, the communications or activities subject to surveillance, the type of electronic surveillance used, and whether physical entry is needed. 50 U.S.C. § 1805(d).

Such an order may approve an electronic surveillance for the period of time necessary to achieve its purpose or for ninety days, whichever is less, unless the order

---

[36] 50 U.S.C. § 1805(c). The italics in 50 U.S.C. § 1805(c)(2)(B), above, indicates new language added by Section 206 of P.L. 107-56. Where circumstances suggest that a target's actions may prevent identification of a specified person, this new language appears to permit the Foreign Intelligence Surveillance Court to require a service provider, other common carrier, landlord, custodian or other persons to provide necessary assistance to the applicant for a FISA order for electronic surveillance. The heading to Section 6 of P.L. 107-56 refers to this as "roving surveillance authority." H.Rept. 107-328 calls this a "multipoint" wiretap. *Intelligence Authorization Act for Fiscal Year 2002*, 107th Cong., 1st Sess., H.Rept. 107-328, Conference Report, at 24 (Dec. 6, 2001).

is targeted against a foreign power. In that event, the order shall approve an electronic surveillance for the period specified in the order or for one year, whichever is less. An order under FISA for surveillance targeted against an agent of a foreign power who acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor, may be for the period specified in the order or 120 days, whichever is less.[37] Generally, upon application for an extension, a court may grant an extension of an order on the same basis as an original order. An extension must include new findings made in the same manner as that required for the original order. However, an extension of an order for a surveillance targeting a foreign power that is not a United States person may be for a period of up to one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period involved. In addition, an extension of an order for surveillance targeted at an agent of a foreign power who acts in the United States as an officer or employee of a foreign power or as a member of a group engaged in international terrorism or activities in preparation therefore may be extended to a period not exceeding one year. 50 U.S.C. § 1805(e)(2)(A) and (B).[38]

---

[37] 50 U.S.C. § 1805(e)(1)(B), as added by Section 207 of P.L. 107-56.

[38] Section 207 of P.L. 107-56 appears to have included a mistaken citation here, referring to 50 U.S.C. § *1805(d)(2)* instead of 50 U.S.C. § *1805(e)(2)* (emphasis added). The amending statutory language discussed above appears to reflect an intended change to subsection 1805(e)(2), as there is no existing statutory language readily susceptible to such an amendment in subsection 1805(d)(2). Section 314(c)(1) of P.L. 107-108, the conference version of H.R. 2883, in H.Rept. 107-328, corrected the apparent error from P.L. 107-56, Section 207, so that the reference is now to 50 U.S.C. § 1805(e)(2). The conference version of H.R. 2883 was signed into law by the President on December 28, 2001.

Emergency situations are addressed in 50 U.S.C. § 1805(f).[39] Notwithstanding other provisions of this subchapter, if the Attorney General reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained and that the factual basis for issuance of an order under this subchapter to approve such surveillance exists, he may authorize electronic surveillance if specified steps are taken. At the time of the Attorney General's emergency authorization, he or his designee must inform an FISC judge that the decision to employ emergency electronic surveillance has been made. An application for a court order under Section 1804 must be made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes emergency electronic surveillance, he must require compliance with the minimization procedures required for the issuance of a judicial order under this subchapter. Absent a judicial order approving the emergency electronic surveillance, the surveillance must terminate when the information sought is obtained, when the application for the order is denied, or after 72 hours from the time of the Attorney General's authorization, whichever is earliest.[40] If no judicial order approving the surveillance is issued, the information

---

[39] 50 U.S.C. § 1805(g) authorizes officers, employees, or agents of the United States to conduct electronic surveillance in the normal course of their official duties to test electronic equipment, determine the existence and capability of equipment used for unauthorized electronic surveillance, or to train intelligence personnel in the use of electronic surveillance equipment. Under 50 U.S.C. § 1805(h), the certifications of the Attorney General pursuant to 50 U.S.C. § 1802(a) and applications made and orders granted for electronic surveillance under FISA must be retained for at least 10 years.

Section 225 of P.L. 107-56 appears to create a second subsection 1805(h), which precludes any cause of action in any court "against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance" under FISA. This immunity provision is included in 50 U.S.C. § 1805, and was denominated "Immunity for Compliance with FISA Wiretap" in Section 225 of the USA PATRIOT Act, both facts which might lead one to conclude that it applied only to electronic surveillance under FISA. However, in H.Rept. 107-328, the conference report accompanying H.R. 2883, which became P.L. 107-108, the conferees expressed the view that "the text of section 225 refers to court orders and requests for emergency assistance 'under this act,' which makes clear that it applies to physical searches (and pen-trap requests–for which there already exists an immunity provision, 50 U.S.C. § 1842(f)–and subpoenas) as well as electronic surveillance." *Id.* at 25.

Section 314(a)(2)(C) of P.L. 107-108, the conference report version of H.R. 2883, in H.Rept. 107-328, changed subsection (h), which was added to 50 U.S.C. § 1805 by Section 225 of P.L. 107-56, to subsection (i). In addition, Section 314(a)(2)(D) of the conference report version of H.R. 2883 added "for electronic surveillance or physical search" to the end of the newly designated 50 U.S.C. § 1805(i) before the final period. The measure was signed into law by the President on December 28, 2001.

[40] Section 314(a)(2)(B) of the conference report version of H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002, H.Rept. 107-328, replaced 24 hours with 72 hours

(continued...)

garnered may not be received in evidence or otherwise disclosed in any court proceeding, or proceeding in or before any grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof. No information concerning any United States person acquired through such surveillance may be disclosed by any Federal officer or employee without the consent of that person, unless the Attorney General approves of such disclosure or use where the information indicates a threat of death or serious bodily harm to any person.[41]

---

[40] (...continued)
in each place that it appears in 50 U.S.C. § 1805(f). The measure was forwarded to the President for his signature on December 18, 2001, and signed into law on December 28, 2001, as P.L. 107-108.

[41] Some of the provisions dealing with interception of wire, oral, or electronic communications in the context of criminal law investigations, 18 U.S.C. §§ 2510 *et seq.*, may also be worthy of note. With certain exceptions, these provisions, among other things, prohibit any person from engaging in intentional interception; attempted interception; or procuring others to intercept or endeavor to intercept wire, oral, or electronic communication; or intentional disclosure; attempting to disclose; using or endeavoring to use the contents of a wire, oral or electronic communication, knowing or having reason to know that the information was obtained by such an unlawful interception. 18 U.S.C. § 2511. "Person" is defined in 18 U.S.C. § 2510(6) to include "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." Among the exceptions to Section 2511 are two of particular note:

> (2)(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.
>
> (2)(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

Among other things, Section 2512 prohibits any person from intentionally manufacturing, assembling, possessing, or selling any electronic, mechanical, or other device, knowing that its design renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. It also prohibits any person from intentionally sending such a device through the mail or sending or carrying such a device in interstate or foreign commerce, knowing that such surreptitious interception is its primary purpose. Similarly,
(continued...)

[41] (...continued)
intentionally advertising such a device, knowing or having reason to know that the advertisement will be sent through the mail or transported in interstate or foreign commerce is foreclosed. Again an exception to these general prohibitions in Section 2512 may be of particular interest:

> (2) It shall not be unlawful under this section for—
> (a) . . .
> (b) an officer, agent, or employee of, or a person under contract with, the United States . . . in the normal course of the activities of the United States . . .,
> to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

In addition, Section 107 of the Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1858, October 21, 1986, [which enacted 18 U.S.C. §§ 1367, 2621, 2701 to 2711, 3117, and 3121 to 3126; and amended 18 U.S.C. §§ 2232, 2511-2513, and 2516-2520], provided generally that, "[n]othing in this act or the amendments made by this act constitutes authority for the conduct of any intelligence activity." It also stated:

> (b) Certain Activities Under Procedures Approved by the Attorney General.–Nothing in chapter 119 [interception of wire, oral or electronic communications] or chapter 121 [stored wire and electronic communications and transactional records access] of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to--
> (1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;
> (2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.]; or
> (3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.].

In addition, Chapter 121 of title 18 of the United States Code deals with stored wire and electronic communications and transactional records. Under 18 U.S.C. § 2701, intentionally accessing without authorization a facility through which an electronic communication service is provided, or intentionally exceeding an authorization to access such a facility and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage in such system is prohibited. Upon compliance with statutory requirements in 18 U.S.C. § 2709, the Director of the FBI or his designee in a position not lower than deputy Assistant Director may seek access to telephone toll and transactional records for foreign counterintelligence purposes. The FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the FBI, and, "with respect to dissemination

(continued...)

The uses to which information gathered under FISA may be put are addressed under 50 U.S.C. § 1806.[42] Under these provisions, disclosure, without the

---

[41] (...continued)
to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency." 18 U.S.C. § 2709(d).

[42] The provisions of Section 1806 are as follows:

> (a) Compliance with minimization procedures; privileged communications; lawful purposes
>
> Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with or in violation of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.
>
> (b) Statement for disclosure
>
> No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.
>
> (c) Notification by United States
>
> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.
>
> (d) Notification by States or political subdivisions
>
> Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof intends to so disclose or so use such information.
>
> (e) Motion to suppress
>
> Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(continued...)

[42] (...continued)

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(continued...)

consent of the person involved, of information lawfully acquired under FISA which concerns a United States person must be in compliance with the statutorily mandated minimization procedures. Communications which were privileged when intercepted remain privileged. Where information acquired under FISA is disclosed for law enforcement purposes, neither that information nor any information derived therefrom may be used in a criminal proceeding without prior authorization of the Attorney General. If the United States Government intends to disclose information acquired under FISA or derived therefrom in any proceeding before a court, department, officer

---

[42] (...continued)

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application or on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forgo ordering the serving of the notice required under this subsection.

(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers *or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)* to coordinate efforts to investigate or protect against–

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) [50 U.S.C. § 1804(a)(7)(B) (referring to a certification by the Assistant to the President for National Security Affairs or other designated certifying authority "that a significant purpose of the surveillance is to obtain foreign intelligence information")] or the entry of an order under section 105 [50 U.S.C. § 1805].

(Emphasis added.) Subsection 1806(k) was added by Section 504 of P.L. 107-56. The italicized portion of subsection 1806(k)(1), above, was added by Section 898 of the Homeland Security Act of 2002, P.L. 107-296. The term "aggrieved person," as used in connection with electronic surveillance under FISA, is defined under 50 U.S.C. § 1801(k) to mean "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."

o

regulatory body or other authority of the United States against an aggrieved person,[43] then the Government must give prior notice of its intent to disclose to the aggrieved person and to the court or other authority involved. Similarly, a State or political subdivision of a State that intends to disclose such information against an aggrieved person in a proceeding before a State or local authority must give prior notice of its intent to the aggrieved person, the court or other authority, and the Attorney General.[44]

---

[43] For the definition of "aggrieved person" as that term is used with respect to targets of electronic surveillance under FISA, see fn. 42, *supra*.

[44] It is worthy of note that Section 892 of the Homeland Security Act of 2002, P.L. 107-296, while not expressly amending FISA, addressed procedures for the sharing of homeland security information. It required the President to prescribe and implement procedures under which relevant federal agencies, including those in the intelligence community, would share relevant and appropriate homeland security information with other federal agencies and, where appropriate, with State and local personnel. Section 892 provided, in part:

> Sec. 892. Facilitating Homeland Security Information Sharing Procedures.
>
> (a) Procedures for Determining Extent of Sharing of Homeland Security Information.–
>
> (1) The President shall prescribe and implement procedures under which relevant Federal agencies–
>
> (A) share relevant and appropriate homeland security information with other Federal agencies, including the Department, and appropriate State and local personnel;
>
> (B) identify and safeguard homeland security information that is sensitive but unclassified; and
>
> (C) to the extent that such information is in classified form, determine whether, how, and to what extent to remove classified information, as appropriate, and with which such personnel it may be shared after such information is removed.
>
> (2) The President shall ensure that such procedures apply to all agencies of the Federal Government.
>
> (3) Such procedures shall not change the substantive requirements for the classification and safeguarding of classified information.
>
> (4) Such procedures shall not change the requirements and authorities to protect sources and methods.
>
> (b) Procedures for Sharing of Homeland Security Information.–
>
> (1) Under procedures prescribed by the President, all appropriate agencies, including the intelligence community, shall, through information sharing systems, share homeland security information with Federal agencies and appropriate State and local personnel to the extent such information may be shared, as determined in accordance with subsection (a), together with assessments of the credibility of such information.
>
> (2) Each information sharing system through which information is shared under paragraph (1) shall–
>
> (A) have the capability to transmit unclassified or classified information, though the procedures and recipients for each capability may differ;
>
> (B) have the capability to restrict delivery of information to

(continued...)

Section 1806 also sets out in camera and ex parte district court review procedures to be followed where such notification is received, or where the aggrieved

---

[44] (...continued)

specified subgroups by geographic location, type of organization, position of a recipient within an organization, or a recipient's need to know such information;

(C) be configured to allow the efficient and effective sharing of information; and

(D) be accessible to appropriate State and local personnel.

(3) The procedures prescribed in paragraph (1) shall establish conditions on the use of information shared under paragraph (1)–

(A) to limit the redissemination of such information to ensure that such information is not used for an unauthorized purpose;

(B) to ensure the security and confidentiality of such information;

(C) to protect the constitutional and statutory rights of any individuals who are subjects of such information; and

(D) to provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

(4) . . . .

(5) Each appropriate Federal agency, as determined by the President, shall have access to each information sharing system through which information is shared under paragraph (1), and shall therefore have access to all information, as appropriate, shared under such paragraph.

(6) The procedures prescribed under paragraph (1) shall ensure that appropriate State and local personnel are authorized to use such information systems–

(A) to access information shared with such personnel; and

(B) to share, with others who have access to such information sharing systems, the homeland security information of their own jurisdictions, which shall be marked appropriately as pertaining to potential terrorist activity.

(7) Under procedures prescribed jointly by the Director of Central Intelligence and the Attorney General, each appropriate Federal agency, as determined by the President, shall review and assess the information shared under paragraph (6) and integrate such information with existing intelligence.

. . . .

Subsection (f)(1) of Section 892 of P.L. 107-296, defined "homeland security information" to mean "information possessed by a Federal, State, or local agency" that "relates to the threat of terrorist activity;" "relates to the ability to prevent, interdict, or disrupt terrorist activity;" "would improve the identification or investigation of a suspected terrorist or terrorist organization;" "or would improve the response to a terrorist act." "State and local personnel" is defined to mean persons involved in prevention, preparation, or response for terrorist attack who fall within the following categories: "State Governors, mayors, and other locally elected officials;" "State and local law enforcement personnel and firefighters;" "public health and medical professionals;" "regional, State, and local emergency management agency personnel, including State adjutant generals;" "other appropriate emergency response agency personnel;" and "employees of private-sector entities that affect critical infrastructure, cyber, economic, or public health security, as designated by the Federal Government in procedures developed pursuant to this section."

person seeks to discover or obtain orders or applications relating to FISA electronic surveillance, or to discover, obtain, or suppress evidence or information obtained or derived from the electronic surveillance, and the Attorney General files an affidavit under oath that such disclosure would harm U.S. national security. The focus of this review would be to determine whether the surveillance was lawfully conducted and authorized. Only where needed to make an accurate determination of these issues does the section permit the court to disclose to the aggrieved person, under appropriate security measures and protective orders, parts of the application, order, or other materials related to the surveillance. If, as a result of its review, the district court determines that the surveillance was unlawful, the resulting evidence must be suppressed.[45] If the surveillance was lawfully authorized and conducted, the motion of the aggrieved person must be denied except to the extent that due process requires discovery or disclosure. Resultant court orders granting motions or requests of the aggrieved person for a determination that the surveillance was not lawfully conducted or authorized and court orders requiring review or granting disclosure are final orders binding on all Federal and State courts except a U.S. Court of Appeals and the U.S. Supreme Court.

---

[45] *But see*, United States v. Thomson, 752 F. Supp. 75, 77 (W.D. N.Y. 1990), stating that,

> If the Court determines that the surveillance was unlawfully authorized or conducted, it must order disclosure of the FISA material. 50 U.S.C. § 1806(g) .... In *United States v. Belfield*, 692 F.2d 141 (D.C. Cir. 1982), the court stated that "even when the government has purported not to be offering any evidence obtained or derived from the electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the FISA surveillance material to ensure that no fruits thereof are being used against him." Id. at 146.

It may be noted that the Section 1806(g) does not state that a court must order disclosure of the FISA material if the court finds that the FISA electronic surveillance was unlawfully authorized or conducted. Rather, the provision in question states in pertinent part that, "If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. . . ." While a district court will normally consider in camera and ex parte a motion to suppress under Subsection 1806(e) or other statute or rule to discover, disclose, or suppress information relating to a FISA electronic surveillance, Subsection 1806(f) does permit a district court, in determining the legality of a FISA electronic surveillance, to disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance only to the extent necessary to make an accurate determination of the legality of the surveillance. *Belfield* indicated that a criminal defendant may seek to discover FISA surveillance material to ensure that no fruits of an illegal surveillance are being used against him, but it appears to stop short of saying that in every instance where the court finds an illegal surveillance disclosure must be forthcoming. "The language of section 1806(f) clearly anticipates that an ex parte, in camera determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary." *Belfield, supra*, 692 F.2d at 147. *See also*, United States v. Squillacote, 221 F.3d 542, 552-554 (4th Cir. 2000), *cert. denied*, ___ U.S. ___, 2001 U.S. LEXIS 2915 (April 16, 2001).

If the contents of any radio communication are unintentionally acquired by an electronic, mechanical, or other surveillance device in circumstances where there is a reasonable expectation of privacy and where a warrant would be required if the surveillance were to be pursued for law enforcement purposes, then the contents must be destroyed when recognized, unless the Attorney General finds that the contents indicate a threat of death or serious bodily harm to any person.

As noted above, Section 1805 provides for emergency electronic surveillance in limited circumstances, and requires the subsequent prompt filing of an application for court authorization to the FISC in such a situation. Under Section 1806, if the application is unsuccessful in obtaining court approval for the surveillance, notice must be served upon any United States person named in the application and such other U.S. persons subject to electronic surveillance as the judge determines, in the exercise of his discretion, is in the interests of justice. This notice includes the fact of the application, the period of surveillance, and the fact that information was or was not obtained during this period. Section 1806 permits postponement or suspension of service of notice for up to ninety days upon ex parte good cause shown. Upon a further ex parte showing of good cause thereafter, the court will forego ordering such service of notice.[46]

P.L. 107-56, Section 504, added a new subsection 1806(k)(1). Under this new subsection, federal officers who conduct electronic surveillance to acquire foreign intelligence under FISA are permitted to consult with Federal law enforcement officers to coordinate investigative efforts or to protect against–

> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

---

[46] *Cf., United States Attorney's Manual*, §§ 1-2.106 (Office of Intelligence Policy and Review organization and functions). This section indicates, in part, that the Office of Intelligence Policy and Review

> . . . prepares certifications and applications for electronic surveillance under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., and represents the United States before the United States Foreign Intelligence Surveillance Court. It processes requests for Attorney General Authority to use FISA material in adjudicatory proceedings and assists in responding to challenges to the legality of FISA surveillances.

See also, 28 C.F.R. §§ 0.33a-0.33c (regarding Counsel for Intelligence Policy); *United States Attorneys' Criminal Resource Manual*, §§ 9-1073, 9-1075, 9-1076, 9-1077, 9-1079 (regarding FISA–50 U.S.C. § 1809); *United States Attorneys' Manual* §§ 9-60.400 (regarding criminal sanctions against illegal electronic surveillance under FISA, 50 U.S.C. § 1809); 9-90.210 (contacts with the Intelligence Community regarding criminal investigations or prosecutions).

This new subsection indicates further that such coordination would not preclude certification as required by 50 U.S.C. § 1804(a)(7)(B) or entry of a court order under 50 U.S.C. § 1805.

Reporting requirements are included in Sections 1807 and 1808. Under Section 1807, each year in April, the Attorney General is directed to transmit to the Administrative Office of the United States Courts and to the Congress a report covering the total number of applications made for orders and extensions of orders approving electronic surveillance under FISA during the previous year, and the total number of orders and extensions granted, modified, or denied during that time period. Section 1808(a) requires the Attorney General to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence semiannually about all electronic surveillance under FISA.[47] Each such report must contain a description of each criminal case in which information acquired under FISA "has been passed for law enforcement purposes" during the period covered by the report, and each criminal case in which information acquired under FISA has been authorized to be used at trial during the reporting period.[48]

Section 1809 provides criminal sanctions for intentionally engaging in electronic surveillance under color of law except as authorized by statute; or for disclosing or using information obtained under color of law by electronic surveillance, knowing or having reason to know that surveillance was not authorized by statute.[49] The provision makes it a defense to prosecution under this subsection if the defendant is a law enforcement officer or investigative officer in the course of his official duties and the electronic surveillance was authorized by and conducted under a search

---

[47] Subsection 1808(b) directed these committees to report annually for five years after the date of enactment to the House and the Senate respectively concerning implementation of FISA, including any recommendations for amendment, repeal, or continuation without amendment. P.L. 106-567, Title VI, Sec. 604(b) (Dec. 27, 2000), 114 Stat. 2853, required the Attorney General to submit to the Senate Select Committee on Intelligence, the Senate Judiciary Committee, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee a report on the authorities and procedures utilized by the Department of Justice to determine whether or not to disclose information acquired under FISA for law enforcement purposes. 50 U.S.C. § 1806 note.

[48] 50 U.S.C. § 1808(a)(2).

[49] Section 1075 of the *United States Attorneys' Criminal Resource Manual* indicates that Section 1809(a) "reaches two distinct acts: (1) engaging in unauthorized electronic surveillance under color of law; and (2) using or disclosing information obtained under color of law through unauthorized electronic surveillance. Each offense involves an 'intentional' state of mind and unauthorized 'electronic surveillance.'" Section 1075 further notes:

> Even though none of these elements mentions foreign intelligence, one court has explained that "the FISA applies only to surveillance designed to gather information relevant to foreign intelligence." *United States v. Koyomejian*, 970 F. 2d 536, 540 (9th Cir. 1992) (en banc), cert denied, 506 U.S. 1005 (1992). In fact, all applications for an order from the Foreign Intelligence Surveillance Court require a certification from a presidentially designated official that the purpose of the surveillance is to obtain foreign intelligence. 50 U.S.C. § 1804(a)(7).

warrant or court order of a court of competent jurisdiction. Section 1809 provides for Federal jurisdiction over such an offense if the defendant is a Federal officer or employee at the time of the offense. Civil liability is also provided for under Section 1810, where an aggrieved person, who is neither a foreign power nor an agent of a foreign power, has been subjected to electronic surveillance, or where information gathered by electronic surveillance about an aggrieved person has been disclosed or used in violation of Section 1809.

Finally, Section 1811 provides that, notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order to acquire foreign intelligence information for up to 15 calendar days following a declaration of war by Congress.

Physical searches for foreign intelligence gathering purposes. Physical searches for foreign intelligence purposes are addressed in 50 U.S.C. § 1821 *et seq.*[50] While tailored for physical searches, the provisions in many respects follow a pattern similar to that created for electronic surveillance. The definitions from 50 U.S.C. § 1801 for the terms "foreign power," "agent of a foreign power," "international terrorism," "sabotage," "foreign intelligence information," "Attorney General," "United States person," "United States," "person," and "State" also apply to foreign intelligence physical searches except where specifically provided otherwise. A "physical search" under this title means:

> any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 1801(f) of this title [50 U.S.C.], or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 1801(f) of this title.[51]

Minimization procedures also apply to physical searches for foreign intelligence purposes. Those defined under 50 U.S.C. § 1821(4) are tailored to such physical searches, and like those applicable to electronic surveillance under 50 U.S.C. § 1801(h), these procedures are designed to minimize acquisition and retention, and to prohibit dissemination of nonpublicly available information concerning unconsenting

---

[50] The physical search provisions of FISA were added as Title III of that act by P.L. 103-359, Title VIII, on October 14, 1994, 108 Stat. 3443. Some of these provisions were subsequently amended by P.L. 106-567, Title VI, on December 27, 2000, 114 Stat. 2852-53; and by P.L. 107-56.

[51] 50 U.S.C. § 1821(5).

U.S. persons, consistent with the needs of the United States to obtain, produce and disseminate foreign intelligence.[52]

Under 50 U.S.C. § 1822, the President, acting through the Attorney General may authorize physical searches to acquire foreign intelligence information without a court order for up to one year if the Attorney General certifies under oath that the search is solely directed at premises, property, information or materials owned by or under the open and exclusive control of a foreign power or powers.[53] For these purposes, "foreign power or powers" means a foreign government or component of a foreign government, whether or not recognized by the United States, a faction of a foreign nation or nations, not substantially composed of U.S. persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.[54] In addition, the Attorney General must certify that there is no substantial likelihood that the physical search will involve the premises, information, material or property of a U.S. person, and that the proposed minimization procedures with respect to the physical search are

---

[52] Specifically, 50 U.S.C. § 1821(4) defines "minimization procedures" with respect to physical search to mean:

> (A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> (B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand such foreign intelligence information or assess its importance;
> (C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
> (D) notwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 1822(a) of this title, procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours, unless a court order under section 1824 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Section 314(a)(3) of P.L. 107-108, the conference version of the Intelligence Authorization Act of 2002, H.R. 2883, from H.Rept. 107-328, changed the previous 24 hour period in the minimization procedures under 50 U.S.C. § 1821(4)(D) to a 72 hour period. The bill passed both houses of Congress and was signed by the President on December 28, 2001.

[53] The president provided such authority to the Attorney General by Executive Order 12949, Section 1, 60 *Fed. Reg.* 8169 (February 9, 1995), if the Attorney General makes the certifications necessary under 50 U.S.C. § 1822(a)(1).

[54] *See* 50 U.S.C. § 1801(a)(1), (2), or (3).

consistent with 50 U.S.C. § 1821(4)(1)-(4).[55] Under normal circumstances, these minimization procedures and any changes to them are reported to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence by the Attorney General at least 30 days before their effective date. However, if the Attorney General determines that immediate action is required, the statute mandates that he advise these committees immediately of the minimization procedures and the need for them to become effective immediately. In addition, the Attorney General must assess compliance with these minimization procedures and report such assessments to these congressional committees.

The certification of the Attorney General for a search under 50 U.S.C. § 1822 is immediately transmitted under seal to the Foreign Intelligence Surveillance Court, and maintained there under security measures established by the Chief Justice of the United States with the Attorney General's concurrence, in consultation with the Director of Central Intelligence. Such a certification remains under seal unless one of two circumstances arise: (1) either an application for a court order with respect to the physical search is made to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1821(4) (dealing with minimization procedures) and § 1823 (dealing with the process by which a federal officer, with the approval of the Attorney General, may apply for an order from the FISC approving a physical search for foreign intelligence gathering purposes); or (2) the certification is needed to determine the legality of a physical search under 50 U.S.C. § 1825 (dealing with use of the information so gathered).

In connection with physical searches under 50 U.S.C. § 1822, the Attorney General may direct a landlord, custodian or other specified person to furnish all necessary assistance needed to accomplish the physical search in a way that would both protect its secrecy and minimize interference with the services such person provides the target of the search. Such person may also be directed to maintain any records regarding the search or the aid provided under security procedures approved by the Attorney General and the Director of Central Intelligence. The provision of any such aid must be compensated by the Government.[56] As in the case of applications for electronic surveillance under FISA, the Foreign Intelligence Surveillance Court (FISC) has jurisdiction to hear applications and grant applications with respect to physical searches under 50 U.S.C. § 1821 *et seq.* No FISC judge may hear an application already denied by another FISC judge. If an application for an order authorizing a physical search under FISA is denied, the judge denying the application must immediately provide a written statement of reasons for the denial. If the United States so moves, the record is then transmitted under seal to the court of review established under 50 U.S.C. § 1803(b). If the court of review determines that the application was properly denied, it, in turn, must provide a written statement of the reasons for its decision, which must be transmitted under seal to the Supreme

---

[55] While this is the citation cross-referenced in Section 1822, it appears that the cross-reference should read 50 U.S.C. § 1821(4)(A)-(D).

[56] 50 U.S.C. § 1822(a)(4).

Court upon petition for certiorari by the United States.[57] Any of the proceedings with respect to an application for a physical search under FISA must be conducted expeditiously, and the record of such proceedings must be kept under appropriate security measures.

The requirements for application for an order for a physical search under FISA are included in 50 U.S.C. § 1823. While tailored to a physical search, the requirements strongly parallel those applicable to electronic surveillance under 50 U.S.C. § 1804(a)(1)-(9).[58] Like Section 1804(a)(7)(B) with respect to required

---

[57] 50 U.S.C. § 1822(c), (d).

[58] Each application for an order approving such a physical search, having been approved by the Attorney General based upon his understanding that the application satisfies the criteria and requirements of 50 U.S.C. § 1821 *et seq.*, must be made by a Federal officer in writing upon oath or affirmation to a FISC judge. Under subsection (a) of Section 1823, the application must include:

> (1) the identity of the Federal officer making the application;
> (2) the authority conferred on the Attorney General by the President and the approval of the Attorney General to make the application;
> (3) the identity, if known, or a description of the search, and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;
> (4) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that–
>
> (A) the target of the physical search is a foreign power or an agent of a foreign power;
> (B) the premises or property to be searched contains foreign intelligence information; and
> (C) the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;
>
> (5) a statement of the proposed minimization procedures;
> (6) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;
> (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate–
>
> (A) that the certifying official deems the information sought to be foreign intelligence information;
> (B) that a significant purpose of the search is to obtain foreign intelligence information;
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
> (E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);
>
> (8) where the physical search involves a search of the residence of a United

(continued...)

certifications for an application for electronic surveillance under FISA, Section 1823(a)(7)(B) was amended by P.L. 107-56, Section 218, to require that the Assistant to the President for National Security Affairs or designated executive branch official[59] certify, among other things, that a significant purpose (rather than "that the purpose") of the physical search is to obtain foreign intelligence information.[60] Section 1823(d) also parallels Section 1804(e) (dealing with requirements for some applications for electronic surveillance under FISA), in that, if requested in writing by the Director of the FBI, the Secretary of Defense, the Secretary of State, or the DCI,[61] the Attorney General must personally review an application for a FISA physical search if the target is one described by Section 1801(b)(2). 50 U.S.C. § 1801(b)(2) deals with targets who knowingly engage in clandestine intelligence gathering activities involving or possibly involving violations of federal criminal laws by or on behalf of a foreign power; targets who, at the direction of an intelligence service or network of a foreign power, engage in other clandestine intelligence activities involving or potentially involving federal crimes by or on behalf of a foreign power; targets who knowingly

---

[58] (...continued)

> States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information; and
> (9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, premises, or property specified in the application, and the action taken on each previous application.

Under Section 1823(b), the Attorney General may require any other affidavit or certification from any other officer in connection with an application for a physical search that he deems appropriate. Under Section 1823(c), the FISC judge to whom the application is submitted may also require that the applicant provide other information as needed to make the determinations necessary under 50 U.S.C. § 1824.

[59] In Section 2 of E.O. 12949, 60 *Fed. Reg.* 8169 (February 9, 1995), the President authorized the Attorney General to approve applications to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1823, to obtain court orders for physical searches for the purpose of collecting foreign intelligence information. In Section 3 of that executive order, the President designated the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence to make the certifications required by 50 U.S.C. § 1823(a)(7), in support of an application for a court order for a physical search for foreign intelligence purposes. None of these officials may exercise this authority to make the appropriate certifications unless he or she is appointed by the President, with the advice and consent of the Senate.

[60] As in the case of the change from "the purpose" to "a significant purpose" in the case of electronic surveillance, the parallel language change in Section 1823 with respect to physical searches may also have the effect of blurring the distinction between physical searches for foreign intelligence purposes and those engaged in for law enforcement purposes.

[61] The authority of these officials to make such a written request is non-delegable except where such official is disabled or unavailable. Each must make provision in advance for delegation of this authority should he or she become disabled or unavailable. 50 U.S.C. § 1823(d)(1)(B) and (C).

engage in sabotage or international terrorism, activities in preparation for sabotage or international terrorism, or activities on behalf of a foreign power; targets who knowingly aid, abet, or conspire with anyone to engage in any of the previously listed categories of activities; or targets who knowingly enter the United States under false identification by or on behalf or a foreign power or who assume a false identity on behalf of a foreign power while present in the United States.[62]

Should the Attorney General, after reviewing an application, decide not to approve it, he must provide written notice of his determination to the official requesting the review of the application, setting forth any modifications needed for the Attorney General to approve it. The official so notified must supervise the making of the suggested modifications if the official deems them warranted. Unless the Attorney General or the official involved is disabled or otherwise unable to carry out his or her respective responsibilities under Section 1823, those responsibilities are non-delegable.

As in the case of the issuance of an order approving electronic surveillance under 50 U.S.C. § 1805(a), certain findings by the FISC judge are required before an order may be forthcoming authorizing a physical search for foreign intelligence information under 50 U.S.C. § 1824(a). Once an application under Section 1823 has been filed, an FISC judge must enter an ex parte order, either as requested or as modified, approving the physical search if the requisite findings are made. These include findings that:

> (1) the President has authorized the Attorney General to approve applications for physical searches for foreign intelligence purposes;
> (2) the application has been made by a Federal officer and approved by the Attorney General;
> (3) on the basis fo the facts submitted by the applicant there is probable cause to believe that–
>
> > (A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
> > (B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;
>
> (4) the proposed minimization procedures meet the definition of minimization contained in this subchapter; and
> (5) the application which has been filed contains all statements and certifications required by section 1823 of this title, and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1823(a)(7)(E) of this title and any other information furnished under section 1823(c) of this title.

Like Section 1805(b) regarding electronic surveillance under FISA, a FISC judge making a probable cause determination under Section 1824 may consider the target's

---

[62] See fn. 21, *supra*.

past activities, plus facts and circumstances pertinent to the target's present or future activities.[63]

As in the case of an order under 50 U.S.C. § 1805(c) with respect to electronic surveillance, an order granting an application for a physical search under FISA must meet statutory requirements in 50 U.S.C. § 1824(c) as to specifications and directions. An order approving a physical search must specify:

> (A) the identity, if known, or a description of the target of the physical search;
> (B) the nature and location of each of the premises of property to be searched;
> (C) the type of information, material, or property to be seized, altered, or reproduced;
> (D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and
> (E) the period of time during which the physical searches are approved; . . . .

In addition, the order must direct:

> (A) that the minimization procedures be followed;
> (B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing to the target of the physical search;
> (C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the search or the aid furnished that such person wishes to retain;
> (D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and
> (E) that the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.[64]

Subsection 1824(d) sets the limits on the duration of orders under this section and makes provision for extensions of such orders if certain criteria are met.[65]

---

[63] 50 U.S.C. § 1824(b).

[64] 50 U.S.C. § 1824(c)(1), (2).

[65] P.L. 107-56, Section 207(a)(2), amended 50 U.S.C. § 1824(d)(1) so that it provided:

> (1) An order under this section may approve a physical search for the period necessary to achieve its purpose, or for *90* days, whichever is less, except that *(A)* an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a) [50 U.S.C. § 1801(b)(1)(A)], for the period specified in the application or for one year, whichever is less, *and (B) an order under this section for a physical search against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C.*

(continued...)

Subsection 1824(e) deals with emergency orders for physical searches. It permits the Attorney General, under certain circumstances, to authorize execution of a physical search if the Attorney General or his designee informs a FISC judge that the decision to execute an emergency search has been made, and an application under 50 U.S.C. § 1821 *et seq.* is made to that judge as soon as possible, within 72 hours[66] after the Attorney General authorizes the search. The Attorney General's decision to authorize such a search must be premised upon a determination that "an emergency situation exists with respect to the execution of a physical search to obtain foreign intelligence information before an order authorizing such search can with due diligence be obtained," and "the factual basis for issuance of an order under this title [50 U.S.C. § 1821 *et seq.*] to approve such a search exists."[67] If such an emergency search is authorized by the Attorney General, he must require that the minimization procedures required for issuance of a judicial order for a physical search under 18 U.S.C. § 1821 *et seq.* be followed.[68] If there is no judicial order for a such a physical search, then the search must terminate on the earliest of the date on which the information sought is obtained, the date on which the application for the order is denied, or the expiration of the 72 hour period from the Attorney General's authorization of the emergency

---

[65] (...continued)

§ 1801(b)(1)(A)] may be for the period specified in the application or for 120 days, whichever is less.

The language in italics reflects the changes made by P.L. 107-56. The 90 day time period reflected in the first sentence replaced earlier language which provided for forty-five days.

Section 207(b)(2) of P.L. 107-56 amended 50 U.S.C. § 1824(d)(2) to provide:

> (2) Extensions of an order issued under this title [50 U.S.C. §§ 1821 et seq.] may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this Act for a physical search targeted against a foreign power, as defined in section 101(a)(5) or (6) [50 U.S.C. § 1801(a)(5) or (6)], or against a foreign power, as defined in section 101(a)(4) [50 U.S.C. § 1801(a)(4)], that is not a United States person, *or against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)],* may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.

(Emphasis added.) Under subsection 1824(d)(3), the judge, at or before the end of the time approved for a physical search or for an extension, or at any time after the physical search is carried out, may review circumstances under which information regarding U.S. persons was acquired, retained, or disseminated to assess compliance with minimization techniques.

[66] Section 314(a)(4) of the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, amended 50 U.S.C. § 1824(e) by striking "24 hours" where it occurred and replacing it with "72 hours."

[67] 50 U.S.C. § 1824(e)(1)(A)(i) and (ii). *See* fn.66, *supra*, regarding substitution of "72 hours" for "24 hours" in Subsection 50 U.S.C. § 1824(e)(3)(C) by P.L. 107-108, Sec. 314(a)(4).

[68] 50 U.S.C. § 1824(e)(2).

search.[69] If an application for approval is denied or if the search is terminated and no order approving the search is issued, then neither information obtained from the search nor evidence derived from the search may be used in evidence or disclosed in any

> . . . trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General, if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 302 [50 U.S.C. § 1822].[70]

Subsection 1824(f) requires retention of applications made and orders granted under 50 U.S.C. § 1821 *et seq.*, for a minimum of 10 years from the date of the application.

Like 50 U.S.C. § 1806 with respect to electronic surveillance under FISA, 50 U.S.C. § 1825 restricts and regulates the uses of information secured under a FISA physical search. Such information may only be used or disclosed by Federal officers or employees for lawful purposes. Federal officers and employees must comply with minimization procedures if they use or disclose information gathered from a physical search under FISA concerning a United States person.[71] If a physical search involving the residence of a United States person is authorized and conducted under 50 U.S.C. § 1824, and at any time thereafter the Attorney General determines that there is no national security interest in continuing to maintain the search's secrecy, the Attorney General must provide notice to the United States person whose residence was searched. This notice must include both the fact that the search pursuant to FISA was conducted and the identification of any property of that person which was seized, altered, or reproduced during the search.[72] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1821 *et seq.*, must be accompanied by a statement that such information and any derivative information may only be used in a criminal proceeding with advance authorization from the Attorney General.[73]

The notice requirements relevant to intended use or disclosure of information gleaned from a FISA physical search or derivative information, are similar to those applicable where disclosure or use of information garnered from electronic surveillance is intended. If the United States intends to use or disclose information gathered during or derived from a FISA physical search in a trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body or other authority of the United States against an aggrieved person, the United States must

---

[69] 50 U.S.C. § 1824(e)(3).

[70] 50 U.S.C. § 1824(e)(4).

[71] 50 U.S.C. § 1825(a).

[72] 50 U.S.C. § 1825(b).

[73] 50 U.S.C. § 1825(c).

first give notice to the aggrieved person, and the court or other authority.[74] Similarly, if a State or political subdivision of a state intends to use or disclose any information obtained or derived from a FISA physical search in any trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body, or other State or political subdivision against an aggrieved person, the State or locality must notify the aggrieved person, the pertinent court or other authority where the information is to be used, and the Attorney General of the United States of its intention to use or disclose the information.[75] An aggrieved person may move to suppress evidence obtained or derived from a FISA physical search on one of two grounds: that the information was unlawfully acquired; or that the physical search was not made in conformity with an order of authorization or approval. Such a motion to suppress must be made before the trial, hearing or other proceeding involved unless the aggrieved person had no opportunity to make the motion or was not aware of the grounds of the motion.[76]

In camera, ex parte review by a United States district court may be triggered by receipt of notice under Subsections 1825(d) or (e) by a court or other authority; the making of a motion to suppress by an aggrieved person under Subsection 1825(f); or the making of a motion or request by an aggrieved person under any other federal or state law or rule before any federal or state court or authority to discover or obtain applications, orders, or other materials pertaining to a physical search authorized under FISA or to discover, obtain, or suppress evidence or information obtained or derived from a FISA physical search. If the Attorney General files an affidavit under oath that disclosure of any adversary hearing would harm U.S. national security, the U.S. district court receiving notice or before whom a motion or request is pending, or, if the motion is made to another authority, the U.S. district court in the same district as that authority, shall review in camera and ex parte the application, order, and such other materials relating to the physical search at issue needed to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. If the court finds it necessary to make an accurate determination of the legality of the search, the court may disclose portions of the application, order, or other pertinent materials to the aggrieved person under appropriate security procedures and protective orders, or may require the Attorney General to provide a summary of such materials to the aggrieved person.[77]

If the U.S. district court makes a determination that the physical search was not lawfully authorized or conducted, then it must "suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person." If, on the other hand, the court finds that the physical search was lawfully authorized or conducted, the motion of the

---

[74] 50 U.S.C. § 1825(d). "Aggrieved person," as defined in 50 U.S.C. § 1821(2), "means a person whose premises, property, information, or material is the target of a physical search or any other person whose premises, property, information, or material was subject to physical search."

[75] 50 U.S.C. § 1825(e).

[76] 50 U.S.C. § 1825(f).

[77] 50 U.S.C. § 1825(g).

aggrieved person will be denied except to the extent that due process requires discovery or disclosure.[78]

If the U.S. district court grants a motion to suppress under 50 U.S.C. § 1825(h); deems a FISA physical search unlawfully authorized or conducted; or orders review or grants disclosure of applications, orders or other materials pertinent to a FISA physical search, that court order is final and binding on all federal and state courts except a U.S. Court of Appeals or the U.S. Supreme Court.[79]

As a general matter, where an emergency physical search is authorized under 50 U.S.C. § 1824(d), and a subsequent order approving the resulting search is not obtained, any U.S. person named in the application and any other U.S. persons subject to the search that the FISC judge deems appropriate in the interests of justice must be served with notice of the fact of the application and the period of the search, and must be advised as to whether information was or was not obtained during that period.[80] However, such notice may be postponed or suspended for a period not to exceed 90 days upon an ex parte showing of good cause to the judge, and, upon further good cause shown, the court must forego such notice altogether.[81]

Section 504(b) of P.L. 107-56, added a new 50 U.S.C. § 1825(k) to the statute, which deals with consultation by federal officers doing FISA searches with federal law enforcement officers. Section 899 of the Homeland Security Act of 2002, P.L. 107-296 expanded this authority to also permit consultation with "law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)." Under this new language, as amended, federal officers "who conduct physical searches to acquire foreign intelligence information" under 50 U.S.C. § 1821 *et seq.*, may consult with federal law enforcement officers or state or local law enforcement personnel:

> . . . to coordinate efforts to investigate or protect against
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.[82]

Such coordination does not preclude certification required under 50 U.S.C. § 1823(a)(7) or entry of an order under 50 U.S.C. § 1824.[83]

---

[78] 50 U.S.C. § 1825(h).

[79] 50 U.S.C. § 1825(i).

[80] 50 U.S.C. § 1825(j)(1).

[81] 50 U.S.C. § 1825(j)(2).

[82] 50 U.S.C. § 1825(k)(1).

[83] 50 U.S.C. § 1825(k)(2).

50 U.S.C. § 1826 provides for semiannual congressional oversight of physical searches under FISA. The Attorney General is directed to "fully inform" the permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate with respect to all physical searches conducted under 50 U.S.C. § 1821 *et seq.* Also on a semiannual basis, the Attorney General is required to provide a report to those committees and to the House and Senate Judiciary Committees setting forth: the total number of applications for orders approving FISA physical searches during the preceding six month period; the total number of those orders granted, modified, or denied; the number of such physical searches involving the residences, offices, or personal property of United States persons; and the number of occasions, if any, the Attorney General gave notice under 50 U.S.C. § 1825(b).[84]

Section 1827 imposes criminal sanctions for intentionally executing a physical search for foreign intelligence gathering purposes under color of law within the United States except as authorized by statute. In addition, criminal penalties attach to a conviction for intentionally disclosing or using information obtained by a physical search under color of law within the United States for the purpose of gathering intelligence information, where the offender knows or has reason to know that the information was obtained by a physical search not authorized by statute. In either case, this section provides that a person convicted of such an offense faces a fine of not more than $10,000,[85] imprisonment for not more than five years or both. Federal jurisdiction attaches where the offense is committed by an officer or employee of the United States. It is a defense to such a prosecution if the defendant was a law enforcement or investigative officer engaged in official duties and the physical search was authorized and conducted pursuant to a search warrant or court order by a court of competent jurisdiction.

In addition, an aggrieved person other than a foreign power or an agent of a foreign power as defined under section 1801(a) or 1801(b)(1)(A),[86] whose premises, property, information, or material within the United States was physically searched under FISA; or about whom information obtained by such a search was disclosed or used in violation of 50 U.S.C. § 1827, may bring a civil action for actual damages, punitive damages, and reasonable attorney's fees and other investigative and litigation costs reasonably incurred.[87]

---

[84] *See* fn. 72, *supra*, and accompanying text.

[85] This section was added in 1994 as Title III, Section 307 of P.L. 95-511, by P.L. 103-359, Title VIII, § 807(a)(3), 108 Stat. 3452. If a fine were to be imposed under the general fine provisions 18 U.S.C. § 3571, rather than under the offense provision, the maximum fine would be $250,000 for an individual.

[86] For definitions, *see* fn. 21, *supra*.

[87] 50 U.S.C. § 1828. Actual damages are defined to be "not less than liquidated damages of $1,000 or $100 per day for each violation, whichever is greater." 50 U.S.C. § 1828(1).

In times of war, the President, through the Attorney General, may authorize physical searches under FISA without a court order to obtain foreign intelligence information for up to 15 days following a declaration of war by Congress.[88]

Pen registers or trap and trace devices[89] used for foreign intelligence gathering purposes. Title IV of FISA, 50 U.S.C. § 1841 *et seq.*, was added in 1998, amended by P.L. 107-56,[90] and amended further by Section 314(5) of P.L. 107-108. Under 50 U.S.C. § 1842(a)(1), notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may apply for an order or extension of an order authorizing or approving the installation and use of a pen register or trap and trace device "*for any investigation to protect against international terrorism or clandestine intelligence activities, provided such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution*" conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to E.O. 12333 or a successor order.[91] This authority is separate from the authority to conduct electronic surveillance under 50 U.S.C. § 1801 *et seq.*[92]

Each such application is made in writing upon oath or affirmation to a FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant orders approving installation of pen registers or trap and trace devices on behalf of a FISC judge. The application must be approved by the Attorney General or a designated attorney for the Government. Each application must identify the federal officer seeking to use the pen register or

---

[88] 50 U.S.C. § 1829.

[89] Under 50 U.S.C. § 1841(2), the terms "pen register" and "trap and trace device" are given the meanings in 18 U.S.C. § 3127. Under Section 3127, "pen register"

> . . . means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; . . . .

As defined by 18 U.S.C. § 3127(4), "trap and trace device" "means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 50 U.S.C. § 1841 is the section that defines terms applicable to the pen register and trap and trace device portions of FISA.

[90] Title IV of FISA was added by Title VI, Sec. 601(2) of P.L. 105-272, on October 20, 1998, 112 Stat. 2405-2410, and amended by P.L. 107-56 and by P.L. 107-108.

[91] The italicized language was added by P.L. 107-56, Section 214(a)(1), replacing language which had read "for any investigation to gather foreign intelligence information or information concerning international terrorism."

[92] 50 U.S.C. § 1842(a)(2).

trap and trace device sought in the application. It must also include a certification by the applicant "*that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.*"[93]

Under 50 U.S.C. § 1842, as amended by P.L. 107-56, pen registers and trap and trace devices may now be installed and used not only to track telephone calls, but also other forms of electronic communication such as e-mail. Once an application is made under Section 1842, the judge[94] must enter an ex parte order[95] as requested or as

---

[93] This language, added by P.L. 107-56, Section 214(a)(2), replaced stricken language which read:

> (2) a certification by the applicant that the information to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General; and
> (3) information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with--
> (A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or
> (B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

[94] This section refers simply to "judge." In light of 50 U.S.C. § 1842(b), it would appear that this may refer to either a FISC judge or a U.S. magistrate judge designated by the Chief Justice under Section 1842(b)(2) to hear applications for and grant orders approving installation and use of pen registers or trap and trace devices on behalf of a FISC judge. The legislative history on this provision does not appear to clarify this point. The language was included in the bill reported out as an original measure by the Senate Select Committee on Intelligence, S. 2052, as Sec. 601. The Committee's report, S. Rept. 105-185, indicates that magistrate judges were included in the legislation to parallel their use in connection with receipt of applications and approval of pen registers and trap and trace devices in the context of criminal investigations, but reflected the Committee's understanding that the authority provided in the legislation to designate magistrate judges to consider applications for pen registers and trap and trace devices in the foreign intelligence gathering context would be closely monitored by the Department of Justice and this designation authority would not be exercised until the Committee was briefed on the compelling need for such designations, as reflected, for example, through statistical information on the frequency of applications to the FISC under the new procedure. S. Rept. 105-185, at 28 (May 7, 1998). The provision creating on pen registers and trap and trace devices in foreign intelligence and international terrorism investigations, Sec. 601 of the bill as passed, was among those included in the conference version of H.R. 3694 which was passed in lieu of S. 2052. H. Conference Rept. 105-80, at 32 (October 5, 1998).

[95] Under 50 U.S.C. § 1842(d)(2)(A), such an order

(continued...)

modified approving the installation and use of a pen register or trap and trace device if the application meets the requirements of that section.

---

[95] (...continued)

(A) shall specify--

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(iii) the attributes of the communications to which the order applies, such as the number or other identifies, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.

(B) shall direct that--

(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;

(ii) such provider, landlord, custodian, or other person--

(I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and

(II) shall maintain, under security procedures approved by the Attorney General and the Director of Central Intelligence pursuant to section 1805(b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; and

(iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance.

The italicized portions of this section reflect amended language from P.L. 107-56, Section 214 (a)(4).

P.L. 107-108, Section 314(a)(5)(B), replaced "of a court" at the end of 50 U.S.C. § 1842(f) with "of an order issued," so that the language now reads:

(f) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance with the terms *of an order issued* under this section.

(Emphasis added.) *Cf.*, 50 U.S.C. § 1805(f), which contains an immunity grant which, at first blush would appear to apply only to electronic surveillance under FISA, but which has been interpreted in H.Rept. 107-328, page 25, the conference committee accompanying H.R. 2883, which became P.L. 107-108, to apply to electronic surveillance, physical searches and pen register and trap and trace devices. See discussion at fn. 39, *supra.*

Section 1843 of Title 18 of the United States Code focuses upon authorization for installation and use of a pen register or trap and trace device under FISA during specified types of emergencies. This provision applies when the Attorney General makes a reasonable determination that:

> (1) an emergency requires the installation and use of a pen register or trap and trace device to obtain *foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of a activities protected by the first amendment to the Constitution* before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and
> (2) the factual basis for issuance of an order under section 1842(c) of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.[96]

Upon making such a determination, the Attorney General may authorize the installation and use of a pen register or trap and trace device for this purpose if two criteria are met. First, the Attorney General or his designee must inform a judge referred to in Section 1842(b)[97] at the time of the emergency authorization that the decision to install and use the pen register or trap and trace device has been made. Second, an application for a court order authorizing a pen register or trap and trace device under 50 U.S.C. § 1842(a)(1) must be made to the judge as soon as practicable, but no later that 48 hours after the emergency authorization.[98] If no order approving the installation and use of a pen register or trap and trace device is forthcoming, then the installation and use of such pen register or trap and trace device must terminate at the earlier of the time when the information sought is obtained, the time when the application for the order is denied under 50 U.S.C. § 1842, or the expiration of 48 hours from the time the Attorney General made his emergency authorization.[99]

If an application for an order sought under Section 1843(a)(2) is denied, or if the installation and use of the pen register or trap and trace device is terminated, and no order approving it is issued under 50 U.S.C. § 1842(b)(2), then no information obtained or evidence derived from the use of the pen register or trap and trace device may be received in evidence or disclosed in any trial, hearing or other proceeding in any court, grand jury, department, office, agency, regulatory body, legislative committee or other federal state or local authority. Furthermore, in such circumstances, no information concerning a United States person acquired from the use of the pen register or trap and trace device may later be used or disclosed in any

---

[96] 50 U.S.C. § 1843(b) (italics reflect language added by P.L. 107-56, § 214(b)(2), in place of language which read "foreign intelligence information or information concerning international terrorism.") Similar language was inserted in 50 U.S.C. § 1843(a) by P.L. 107-56, § 214(b)(1), in place of language that paralleled that stricken from subsection 1843(b).

[97] See discussion of the term "judge" as used in Section 1842(b) in fn. 94, *supra.*

[98] 50 U.S.C. § 1843(a).

[99] 50 U.S.C. § 1843(c)(1).

other way by federal officers or employees without consent of the U.S. person involved, with one exception. If the Attorney General approves the disclosure because the information indicates a threat of death or serious bodily harm to anyone, then disclosure without consent of the U.S. person involved is permitted.[100]

If Congress declares war, then, notwithstanding any other provision of law, the President, through the Attorney General, may authorize use of a pen register or trap and trace device without a court order to acquire foreign intelligence information for up to 15 calendar days after the declaration of war.[101]

50 U.S.C. § 1845 sets parameters with respect to the use of information obtained through the use of a pen register or trap and trace device under 50 U.S.C. § 1841 *et seq.* Federal officers and employees may only use or disclose such information with respect to a U.S. person without the consent of that person in accordance with Section 1845.[102] Any disclosure by a Federal officer or employee of information acquired pursuant to FISA from a pen register or trap and trace device must be for a lawful purpose. [103] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1841 *et seq.* is only permitted where the disclosure is accompanied by a statement that the information and any derivative information may only be used in a criminal proceeding with the advance authorization of the Attorney General.[104]

Under 50 U.S.C. § 1845(c), when the United States intends to enter into evidence, use, or disclose information obtained by or derived from a FISA pen register or trap and trace device against an aggrieved person[105] in any federal trial, hearing, or proceeding, notice requirements must be satisfied. The Government, before the trial, hearing, or proceeding or a reasonable time before the information is to be proffered, used or disclosed, must give notice of its intent both to the aggrieved

---

[100] 50 U.S.C. § 1843(c)(2).

[101] 50 U.S.C. § 1844.

[102] 50 U.S.C. § 1845(a)(1).

[103] 50 U.S.C. § 1845(a)(2).

[104] 50 U.S.C. § 1845(b).

[105] "Aggrieved person" is defined in 50 U.S.C. § 1841(3) for purposes of 50 U.S.C. § 1841 *et seq.* as any person:

> (A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by subchapter IV [50 U.S.C. § 1841 et seq.]; or
> (B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by subchapter IV to capture incoming electronic or other communications impulses.

person involved[106] and to the court or other authority in which the information is to be disclosed or used.

If a state or local government intends to enter into evidence, use, or disclose information obtained or derived from such a trap and trace device against an aggrieved person in a state or local trial, hearing or proceeding, it must give notice to the aggrieved person and to the Attorney General of the United States of the state or local government's intent to disclose or use the information.[107]

The aggrieved person in either case may move to suppress the evidence obtained or derived from a FISA pen register or trap and trace device on one of two grounds: that the information was unlawfully acquired; or that the use of the pen register or trap and trace device was not made in conformity with an order of authorization or approval under 50 U.S.C. 1841 *et seq.*[108]

If notice is given under 50 U.S.C. §§ 1845(c) or (d), or a motion or request is made to suppress or to discover or obtain any applications, orders, or other materials relating to use of a FISA pen register or trap and trace device or information obtained by or derived from such use, the Attorney General may have national security concerns with respect to the effect of such disclosure or of an adversary hearing. If he files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, the United States district court in which the motion or request is made, or where the motion or request is made before another authority, the U.S. district court in the same district, shall review *in camera* and *ex parte* the application, order, and other relevant materials to determine whether the use of the pen register or trap and trace device was lawfully authorized and conducted.[109] In so doing, the court may only disclose portions of the application, order or materials to the aggrieved person or order the Attorney General to provide the aggrieved person with a summary of these materials if that disclosure is necessary to making an accurate determination of the legality of the use of the pen register or trap and trace device.[110]

Should the court find that the pen register or trap and trace device was not lawfully authorized or conducted, it may suppress the unlawfully obtained or derived evidence or "otherwise grant the motion of the aggrieved person."[111] On the other hand, if the court finds the pen register or trap and trace device lawfully authorized

---

[106] The statute refers to notice to the "aggrieved person." Here it is using this term in the context of a pen register or trap and trace device, as defined in 50 U.S.C. § 1841(3) (see fn. 105, *supra).* This term is also defined in both 50 U.S.C. §§ 1801(k) (in the context of electronic surveillance, see fn. 42, *supra*) and 1825(d) (in the context of a physical search, see fn. 74, *supra*).

[107] 50 U.S.C. § 1845(d).

[108] 50 U.S.C. § 1845(e).

[109] 50 U.S.C. § 1845(f)(1).

[110] 50 U.S.C. § 1845(f)(2).

[111] 50 U.S.C. § 1845(g)(1).

and conducted, it may deny the aggrieved person's motion except to the extent discovery or disclosure is required by due process.[112] Any U.S. district court orders granting motions or request under Section 1845(g), finding unlawfully authorized or conducted the use of a pen register or trap and trace device, or requiring review or granting disclosure of applications, orders or other materials regarding installation and use of a pen register or trap and trace device are deemed final orders. They are binding on all federal and state courts except U.S. courts of appeals and the U.S. Supreme Court.[113]

Section 1846 deals with congressional oversight of the use of FISA pen registers and trap and trace devices. It requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence regarding all FISA uses of pen registers and trap and trace devices. In addition, the Attorney General, on a semi-annual basis, must report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee on the total number of applications made for orders approving the use of such pen registers and trap and trace devices and the total number of such orders granted, modified, or denied during the previous six month period.

Access to certain business records for foreign intelligence purposes. Added in 1998, Title V of FISA, 50 U.S.C. § 1861 *et seq.*, was substantially changed by P.L. 107-56 and modified further by P.L. 107-108.[114]

---

[112] 50 U.S.C. § 1845(g)(2).

[113] 50 U.S.C. § 1845(h).

[114] Title V of FISA was added by Title VI, Sec. 602, of P.L. 105-272, on October 20, 1998, 112 Stat. 2411-12, and significantly amended by P.L. 107-56 and P.L. 107-108. The prior version of 50 U.S.C. § 1861 provided definitions for "foreign power," "agent of a foreign power," "foreign intelligence information," "international terrorism," and "Attorney General," "common carrier," "physical storage facility," "public accommodation facility," and "vehicle rental facility" for purposes of 50 U.S.C. § 1861 *et seq*. The prior version of Section 1862 was much more narrowly drawn than the new version added in P.L. 107-56 and amended by P.L. 107-108. The earlier version read:

> (a) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism which investigation is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.
> (b) Each application under this section–
>
> (1) shall be made to–
> (A) a judge of the court established by section 1803(a) of this title; or
> (B) a United States Magistrate Judge under chapter 43 of Title 28 [28
>
> (continued...)

Although denominated "access to certain business records for foreign intelligence and international terrorism investigations," the reach of Section 1861, as amended by the USA PATRIOT Act and P.L. 107-108, is now substantially broader than business records alone. Under 50 U.S.C. § 1861(a)(1), the Director of the FBI, or his designee (who must be at the Assistant Special Agent in Charge level or higher in rank) may apply for an order requiring

> . . . the production of any tangible things (including books, records, papers, documents, and other items) for an investigation *to obtain foreign intelligence information not concerning a United States person or* to protect against international terrorism or clandestine intelligence activities, provided that such

---

[114] (...continued)

> U.S.C. § 631 *et seq.*], who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the release of records under this section on behalf of a judge of that court; and
>
> (2) shall specify that–
>
> (A) the records concerned are sought for an investigation described in subsection (a); and
>
> (B) there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.
>
> (c)(1) Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application satisfied the requirements of this section.
>
> (2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).
>
> (d)(1) Any common carrier, public accommodation facility, physical storage facility, or vehicle rental facility shall comply with an order under subsection (c).
>
> (2) No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof, shall disclose to any person (other than those officers, agents, or employees of such common carrier, public accommodation facility, physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau of Investigation has sought or obtained records pursuant to an order under this section.

Congressional oversight was covered under the prior provisions by 50 U.S.C. §1863, which was similar, but not identical to the new Section 1862. The former Section 1863 stated:

> (a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all request for records under this subchapter [50 U.S.C. § 1861 *et seq.*].
>
> (b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period–
>
> (1) the total number of applications made for orders approving requests for records under this subchapter [50 U.S.C. § 1861 *et seq.*]; and
>
> (2) the total number of such orders either granted, modified, or denied.

> investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[115]

Subsection 1861(a)(2) requires that such an investigation must be conducted under guidelines approved by the Attorney General under E.O. 12333 or a successor order and prohibits such an investigation of a United States person based solely upon First Amendment protected activities.

An application for an order under Section 1861 must be made to an FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant such orders for the production of tangible things on behalf of an FISC judge.[116] The application must specify that the "records"[117] are sought for "an authorized investigation conducted in accordance with [50 U.S.C. § 1862(a)(2)] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine

---

[115] The italicized portion of Section 1861(a)(1) was added by Section 314(a)(6) of P.L. 107-108. H.Rept. 107-328, the conference report to accompany H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), at page 24, describes the purpose of this addition as follows:

> Section 215 of the USA PATRIOT Act of 2001 amended title V of the FISA, adding a new section 501 [50 U.S.C. § 1861]. Section 501(a) now authorizes the director of the FBI to apply for a court order to produce certain records "For an investigation to protect against international terrorism or clandestine intelligence activities." Section 501(b)(2) directs that the application for such records specify that the purpose of the investigation is to "obtain foreign intelligence information not concerning a United States person." However, section 501(a)(1), which generally authorizes the applications, does not contain equivalent language. Thus, subsections (a)(1) and (b)(2) now appear inconsistent.
>
> The conferees agreed to a provision which adds the phrase "to obtain foreign intelligence information not concerning a United States person or" to section 501(a)(1). This would make the language of section 501(a)(1) consistent with the legislative history of section 215 of the USA PATRIOT Act (*see* 147 Cong. Res. S11006 (daily ed. Oct. 25, 2001) (sectional analysis)) and with the language of section 214 of the USA PATRIOT Act (authorizing an application for an order to use pen registers and trap and trace devices to "obtain foreign intelligence information not concerning a United States person.").

[116] 50 U.S.C. § 1861(b)(1).

[117] While the language refers to "records," it is worthy of note that the authority conferred upon the Director of the FBI or his designee under Section 1861(a) encompasses applications for orders requiring production of "any tangible thing (including books, records, papers, documents, and other items)." One might argue, therefore, that for Subsection 1861(a)(1) and Subsection 1861(b)(2) to be read in harmony, a court might interpret "records" more broadly to cover "any tangible thing." On the other hand, if, by virtue of the specific reference in Subsection 1861(a)(1) to "records" as only one of many types of "tangible things," the term "records" in Subsection 1861(b)(2) were to be read narrowly, it might lead to some confusion as to the nature and scope of any specification that might be required where an application seeking production of types of tangible things other than records is involved.

intelligence activities."[118] When such an application is made, the judge must enter an *ex parte* order "as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section."[119] Such an order shall not disclose that it is issued for purposes of an investigation under 50 U.S.C. § 1861(a).[120] Subsection 1861(d) prohibits any person to disclose that the FBI has sought or obtained tangible things under Section 1861, except where the disclosure is made to persons necessary to the production of tangible things involved. Subsection 1861(e) precludes liability for persons who, in good faith, produce tangible things under such a Section 1861 order. It further indicates that production does not constitute a waiver of any privilege in any other proceeding or context.

50 U.S.C. § 1862 deals with congressional oversight. Subsection 1862(a) requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence regarding all request for production of tangible things under Section 1861.[121] Subsection 1862(b) requires the Attorney General to report to the House and Senate Judiciary Committees on the total number of applications for Section 1861 orders for production of tangible things and on the total number of such orders granted, modified, or denied during the previous six months.

New Private Right of Action

In addition to provisions which amended FISA explicitly, other provisions of the USA PATRIOT Act touched upon FISA, at least tangentially. For example, Section 223 of the act, among other things, created a new 18 U.S.C. § 2712. This new section, in part, created an exclusive private right of action for any person aggrieved by any willful violation of sections 106(a), 305(a), or 405(a) of FISA (50 U.S.C. §§ 1806(a), 1825(a), 1845(a), respectively) to be brought against the United States in U.S. district court to recover money damages. Such monetary relief would amount to either actual damages or $10,000, whichever is greater; and reasonably incurred litigation costs. It also set forth applicable procedures.[122]

---

[118] 50 U.S.C. § 1861(b)(2).

[119] 50 U.S.C. § 1861(c)(1).

[120] 50 U.S.C. § 1861(c)(2).

[121] Section 314(a)(7) of P.L. 107-108 corrected two references in 50 U.S.C. § 1862 as passed in the USA PATRIOT Act. P.L. 107-108 replaced "section 1842 of this title" with "section 1861 of this title," in both places in 50 U.S.C. § 1862 where it appeared.

[122] Another provision, Section 901 of the USA PATRIOT Act, amended 50 U.S.C. § 403-3(c) (Section 103(c) of the National Security Act of 1947) regarding the responsibilities of the Director of Central Intelligence (DCI). The amendment added to those authorities and responsibilities, placing upon the DCI the responsibility for the establishment of

> . . . requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that

(continued...)

USA PATRIOT Act Sunset Provision

Section 224 of the USA PATRIOT Act set a sunset for many of the provisions in the act of December 31, 2005. Among those provisions which will sunset pursuant to this are all of the amendments to FISA, and subsequent amendments thereto, except the provision which increased the number of FISC judges from 7 to 11 (Section 208 of P.L. 107-56). Section 224 also excepts from the application of the sunset provision any particular foreign intelligence investigations that began before December 31, 2005, or any particular offenses or potential offenses which began or occurred before December 31, 2005. As to those particular investigations or offenses, applicable provisions would continue in effect.

Recent Decisions of the FISC and the U.S. Foreign Intelligence Surveillance Court of Review

The FISC Decision

Summary. In its May 17, 2002, decision, the FISC considered a government motion for the court "to vacate the minimization and 'wall' procedures in all cases now or ever before the Court, including this Court's adoption of the Attorney General's July 1995 intelligence sharing procedures, which are not consistent with new intelligence sharing procedures submitted for approval with this motion."[123] The court viewed the new intelligence sharing procedure under review as proposed new Attorney General minimization procedures. In a memorandum and order written by the then Presiding Judge, U.S. District Court Judge Royce Lamberth, issued on the last day of his tenure on the FISC, and concurred in by all of the judges then sitting on the FISC, the FISC granted the Department of Justice (DOJ) motion with significant modifications to section II.B. of the proposed minimization procedures. The court required a continuation of the Attorney General's 1995 minimization procedures, as subsequently modified by the Attorney General and the Deputy Attorney General, and preservation of a "wall" procedure to maintain separation between FBI criminal investigators and DOJ prosecutors and raw FISA investigation data regarding the same facts or individuals, so as to prevent these law enforcement

---

[122] (...continued)
Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that Act unless otherwise authorized by statute or Executive order.

[123] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 613 (U.S. Foreign Intell. Surveil. Ct. 2002).

personnel from becoming "de facto partners in FISA surveillances and searches,"[124] while permitting extensive sharing of information between such investigations.

The FISC was particularly concerned with those aspects of section II.B. of the proposed procedures which would permit criminal prosecutors and law enforcement officers to initiate, direct or control electronic surveillance or physical searches under FISA, with an eye towards law enforcement objectives, rather than foreign intelligence information gathering. The FISC set the stage for its analysis by recounting a significant number of past instances where FISA applications had included false, inaccurate or misleading information regarding information sharing or compliance with "wall" procedures in FBI affidavits or, in one case, in a statutorily required certification by the FBI Director; and past occasions where the FISC's orders had been violated in regard to information sharing and unauthorized dissemination of FISA information to criminal investigators and prosecutors. While both the FBI's and DOJ's Offices of Professional Responsibility had been investigating these incidents for over a year at the time of the writing of the opinion, the court had not been advised of any explanations as to how such misrepresentations had occurred. The court's dissatisfaction with these irregularities formed a backdrop for its analysis of the motion and applications before it.

Discussion of the Memorandum Opinion and Order. Its analysis was based upon its reading of the statutory language and premised, in part, on the fact that the USA PATRIOT Act had not amended the provisions of FISA dealing with minimization requirements, although other FISA provisions had been modified. The minimization provisions with respect to both electronic surveillance and physical searches under FISA continue to be designed to "minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons, consistent with the need of the United States to obtain, produce, and disseminate *foreign intelligence information.*"[125] The court regarded the standard it applied to the proposed procedures before it as "mandated in [50 U.S.C.] § 1805(a)(4) and § 1824(a)(4), which state that 'the proposed minimization procedures meet the definition of minimization procedures under § 101(h), [§ 1801(h) and §1824(4)] of the act.'"

In its memorandum opinion, the FISC first discussed the court's jurisdiction, noting that the text of the statute "leaves little doubt that the collection of foreign

---

[124] *Id.* at 620. In Chapter 3 of *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States* 78-80 (W.W. Norton & Co. 2004) (*Final Report*), the Commission perceived the evolution of the "wall" as a result of statutory language, court interpretation, DOJ interpretation of the legislative language and court decisions, DOJ procedures to manage information sharing between Justice Department prosecutors and the FBI, misunderstanding and misapplication of those procedures, OIPR's stringent exercise of its gate-keeping role, and inaccurate perceptions of field agents. In Chapter 8 of the *Final Report*, at 269-72, the Commission recounted some of the effects of what it saw as the confusion surrounding the rules governing the use and sharing of information of information gathered through intelligence channels.

[125] 50 U.S.C. §§ 1802(h), 1821(4)(A) (emphasis added).

intelligence information is the *raison d'etre* for the FISA."[126] The court found support for this conclusion in a review of pertinent provisions of the act. It found further support in E.O. 12139 and E.O. 12949, which give the Attorney General authority to approve the filing of applications for orders for electronic surveillances and physical searches and authorize the Director of the FBI and other senior executives to make required certifications under FISA for the "purpose of obtaining foreign intelligence information." The FISC therefore concluded that its jurisdiction was limited to granting FISA orders for electronic surveillance and physical searches for the collection of foreign intelligence information under the standards and procedures prescribed in the act.[127] In reaching this conclusion, the FISC, in a footnote, characterized the issue before it as "whether the FISA authorizes electronic surveillance and physical searches *primarily for law enforcement purposes* so long as the Government also has 'a significant' foreign intelligence purpose." Rejecting the approach taken by the Government in its supplemental brief in the case, the Court stated that "its decision is not based on the issue of its jurisdiction but on the interpretation of minimization procedures."[128] Maintaining its focus upon the minimization procedures, the FISC also declined to reach the question raised by the Attorney General "whether FISA may be used primarily for law enforcement purposes."[129]

---

[126] *FISC op.*, 218 F. Supp. 2d at 613. "Foreign intelligence information" is a term of art in FISA, defined in 50 U.S.C. § 1801(e) to mean:

> (e)(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person is necessary to–
> (A) the national defense or the security of the United States; or
> (B) the conduct of the foreign affairs of the United States.

In reaching its decision, the FISC indicated that it was not addressing directly the Department of Justice argument that, so long as a significant purpose of a FISA surveillance or physical search was to gather foreign intelligence information, the primary purpose of such an investigation could be criminal investigation or prosecution. *FISC op.*, 218 F. Supp. 2d at 615 n.2. The FISC was not receptive to the DOJ theory that a "wall" procedure separating a foreign intelligence investigation under FISA from a criminal investigation involving the same target or factual underpinnings was an artificial separation which was not compelled by FISA.

[127] *FISC op.*, 218 F. Supp. 2d at 614.

[128] *Id.* at 614 n.1(emphasis added).

[129] *Id.* at 615 n.2.

The court also regarded the scope of its findings regarding minimization[130] as applicable "only to communications concerning U.S. persons as defined in § 1801(i) of the act: U.S. citizens and permanent resident aliens whether or not they are named targets in the electronic surveillance and physical searches."[131] It emphasized that its opinion was not applicable to communications of foreign powers as defined under 50 U.S.C. § 1801(a), or to non-U.S. persons.[132]

After stating its continued approval of the "Standard Minimization Procedures for a U.S. Person Agent of a Foreign Power," the court turned its attention to two sections of supplementary minimization procedures adopted by the Attorney General

---

[130] FISA defines "minimization procedures" with respect to electronic surveillance in 50 U.S.C. § 1801(h). The term is defined under FISA with respect to physical searches in 50 U.S.C. § 1821(4). As the two definitions are similar, the definition from Section 1801(h) is included for illustrative purposes.

> (h) "Minimization procedures", with respect to electronic surveillance, means–
>
> > (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> > (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
> > (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
> > (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section (1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

[131] *FISC op.*, 218 F. Supp. 2d at 614. This provision defines U.S. persons as follows:

> . . . a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

[132] *Id.*

on March 6, 2002, regarding "II. Intelligence sharing procedures concerning the Criminal Division," and "III. Intelligence sharing procedures concerning a USAO [U.S. Attorney's Office]." The FISC regarded these procedures as minimization procedures as that term is defined under FISA by virtue of the fact that they were adopted by the Attorney General and were "designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[133] Therefore, these procedures were measured against the standard for minimization procedures set forth in 50 U.S.C. §§ 1805(a)(4) and 1824(a)(4):

> . . . The operative language of each section to be applied by the Court provides that minimization procedures must be reasonably designed in light of their purpose and technique, and mean–
>
> > specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, [search] to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. §1801(h)(1) and §1821(4)(A).[134]

The court then reviewed the minimization procedures upon which it had been relying prior to the application before it, to wit, the Attorney General's 1995 "Procedures for Contacts between the FBI and Criminal Division Concerning FI [Foreign Intelligence] and Foreign Counterintelligence Investigations,"as augmented by the Attorney General in January 2000 and expanded further by the Deputy Attorney General in August 2001. The FISC indicated that these procedures permitted the following "substantial consultation and coordination":

a. reasonable indications of significant federal crimes in FISA cases are to be reported to the Criminal Division of the Department of Justice;

b. [t]he Criminal Division may then consult with the FBI and give guidance to the FBI aimed at preserving the option of criminal prosecution, *but may not direct or control* the FISA investigation toward law enforcement objectives;

c. the Criminal Division may consult further with the appropriate U.S. Attorney's Office about such FISA cases;

d. on a monthly basis senior officials of the FBI provide briefings to senior officials of the Justice Department, including OIPR [Office of Intelligence Policy and Review] and the Criminal Division, about intelligence cases, including those in which FISA is or may be used;

e. all FBI 90-day interim reports and annual reports of counterintelligence investigations, including FISA cases, are being provided to the Criminal

---

[133] *Id.* at 616.

[134] *Id.*

Division, and must now contain a section explicitly identifying any possible federal criminal violations;

f. all requests for *initiation or renewal of FISA authority* must now contain a section devoted explicitly to identifying any possible federal criminal *violations*;

g. the FBI is to provide monthly briefings directly to the Criminal Division concerning all counterintelligence investigations in which there is a reasonable indication of a significant federal crime;

h. prior to each briefing the Criminal Division is to identify (from FBI reports) those intelligence investigations about which it requires additional information and the FBI is to provide the information requested; and

i. since September 11, 2001, the requirement that OIPR be present at all meetings and discussions between the FBI and Criminal Division involving certain FISA cases has been suspended; instead, OIPR reviews a daily briefing book to inform itself and this Court about those discussions.[135]

The FISC indicated further that it "routinely approved the use of information screening 'walls' proposed by the government in its applications" to maintain both the appearance and the fact that FISA surveillances and searches were not being used "*sub rosa* for criminal investigations."[136] In March 2000, September 2000, and March 2001, the FISC was advised by the Department of Justice of a significant number of erroneous statements or omissions of material facts in FISA applications, almost all of which involved misstatements or omissions as to information sharing and unauthorized disseminations to criminal investigators and prosecutors.[137] Although the FBI and the Department of Justice Office of Professional Responsibility had been investigating the circumstances involved in these misstatements and omissions for over a year, as of the date of the opinion, the court had not been advised of the reasons for these erroneous statements. The court responded to these concerns in 2001 by instituting supervisory measures to assess compliance with "wall" procedures.

In the case before the FISC here at issue, the government moved that all "wall" procedures be eliminated in international terrorism surveillances and physical searches under FISA. The FISC indicated that the new 2002 procedures proposed by the Attorney General would apply to two types of cases in which "*FISA is the only effective tool available* to both counterintelligence and criminal investigators" (emphasis supplied)–those involving overlapping investigations (which the court described as cases, usually international terrorism cases, in which separate intelligence and criminal investigations of the same FISA target who is a U.S. person

---

[135] *Id.* at 619-20 (emphasis supplied.)

[136] *Id.* at 620.

[137] The September 2000 notification to the FISC from the Department of Justice identified 75 cases of cases involving misstatements or omissions in FISA applications. The court does not indicate the specific number of FISA applications involved in the notifications on the other dates mentioned in the opinion. *See FISC op.*, 218 F. Supp. 2d at 620-21.

are conducted by different FBI agents, where separation can easily be maintained) and those involving overlapping interests (i.e., cases in which one investigation of a U.S. person FISA target is conducted by a team of FBI agents with both intelligence and criminal interests "usually involving espionage and similar cases in which separation is impractical").[138] In both types of investigations, the FISC indicated that the 2002 proposed minimization procedures provided authority for "extensive consultations between the FBI and criminal prosecutors 'to coordinate efforts to investigate or protect against actual or potential attack, sabotage, international terrorism and clandestine intelligence activities by foreign powers and their agents . . . .'" Such consultation is expressly provided for in 50 U.S.C. §§ 1806(k)(1) and 1825(k)(1).

Under the proposed minimization procedures, those consultations would include both providing prosecutors with access to "all information" developed in FBI counterintelligence investigations, including through FISA, among other information. Section II.B. of the proposed minimization techniques would authorize criminal prosecutors to "consult extensively and provide advice and recommendations to intelligence officials about 'all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities.'" The FISC was particularly concerned about the authority given criminal prosecutors under Section II.B. "to advise *FBI intelligence officials concerning 'the initiation, operation, continuation, or expansion of FISA searches or surveillance.'*"[139] The court regarded this provision as "designed to use this Court's orders to enhance criminal investigation and prosecution, consistent with the government's interpretation of the recent amendments that FISA may now be 'used *primarily* for a law enforcement purpose.'"[140] Under section III of the proposed procedures, U.S. attorneys are given the authority to engage in consultations to the same extent as the Criminal Division of DOJ under parts II.A. and II.B. in cases involving international terrorism. The FISC interpreted these procedures as giving criminal prosecutors "a significant role directing FISA surveillances and searches from start to finish in counterintelligence cases involving overlapping intelligence and criminal investigations or interests, guiding them to criminal prosecution."[141]

In light of the court's past experience with FISA searches and surveillances, the FISC found the proposed procedures to be "designed to enhance the acquisition, retention and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information*' (emphasis added [by the FISC]) as mandated in § 1801(h) and § 1821(4)."[142] The court regarded the procedures as, in effect, an effort by the government to amend FISA's definition of minimization procedures in ways that Congress had not and to substitute FISA for the electronic surveillance requirements of Title III of the Omnibus Crime Control and Safe Streets

---

[138] *FISC op.*, 218 F. Supp. 2d at 622.

[139] *Id.* at 623.

[140] *Id.* (Emphasis added).

[141] *Id.*

[142] *Id.*

Act, 18 U.S.C. § 2510 *et seq.*, and for the search warrant requirements in Rule 41 of the Federal Rules of Criminal Procedure. The court found this unacceptable. Nor was the court persuaded by the government's contention that the 1995 procedures' prohibition against criminal prosecutors "directing or controlling" FISA cases should be revoked. "If criminal prosecutors direct both the intelligence and criminal investigations, or a single investigation having combined interests, *coordination becomes subordination* of both investigations or interests to law enforcement objectives."[143]

The FISC stated:

> Advising FBI intelligence officials on the initiation, operation, continuation or expansion of FISA surveillances and searches of U.S. persons means that criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute. The 2002 minimization procedures give the Department's criminal prosecutors every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information, . . . based on a standard that the U.S. person is only using or about to use the places to be surveilled or searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants. All of this may be done by use of procedures intended to minimize collection of U.S. person information, consistent with the need of the United States to obtain and produce foreign intelligence information. If direction of counterintelligence cases involving the use of highly intrusive FISA surveillances and searches by criminal prosecutors is necessary to obtain and produce foreign intelligence information, it is yet to be explained to the Court.[144]

Having found section II.B. of the proposed minimization procedures inconsistent with the statutory standard for minimization procedures under 50 U.S.C. §§ 1801(h) and 1821(4), the court substituted its own language in place of the second and third paragraphs of II.B. as submitted by the Attorney General. The substitute language permitted consultation between the FBI, the Criminal Division of DOJ, and the Office of Intelligence Policy and Review of DOJ (OIPR) "to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or [agents of foreign powers]," so that the goals and objectives of both the intelligence and law enforcement investigations or interests may be achieved. However, it prohibited law enforcement officials from making recommendations to intelligence officials regarding initiation, operation, continuation, or expansion of FISA surveillances and searches. In addition, the substitute language foreclosed law enforcement officials from directing or controlling the use of FISA procedures to enhance criminal prosecution; nor was advice intended to preserve the option of criminal prosecution to be permitted to inadvertently result in the Criminal Division directing or controlling an investigation involving FISA surveillance or physical

---

[143] *Id.* at 623-24 (emphasis in original).

[144] *Id.* at 624.

searches to achieve law enforcement objectives.[145] While direct consultation and coordination were permitted, the substitute language required OIPR to be invited to all such consultations and, where OIPR was unable to attend, the language required OIPR to be apprized forthwith in writing of the substance of the consultations, so that the FISC could be notified at the earliest opportunity.[146]

In its order accompanying the FISC memorandum opinion, the court held that the proposed minimization procedures, so modified, would be applicable to all future electronic surveillances and physical searches under FISA, subject to the approval of the court in each instance.[147] In this order, the court also adopted a new administrative rule to monitor compliance. The new Rule 11 regarding criminal investigations in FISA cases provided:

> All FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office.[148]

The Decision of the U.S. Foreign Intelligence Surveillance Court of Review

Summary. The FISC memorandum opinion and order discussed above were not appealed directly. Rather, the Department of Justice sought review in the U.S. Foreign Intelligence Surveillance Court of Review (Court of Review) of an FISC order which authorized electronic surveillance of an agent of a foreign power, but imposed restrictions on the government flowing from the FISC's May 17th decision, and of an order renewing that surveillance subject to the same restrictions. Because of the electronic surveillance context of these orders, the Court of Review's analysis was cast primarily in terms of such surveillance, although some aspects of its analysis may have broader application to other aspects of FISA. In its first decision ever, the Court of Review, in a lengthy *per curiam* opinion issued on November 18, 2002, reversed and remanded the FISC orders. In so doing the Court of Review emphasized that the May 17th decision, although never appealed, was "the basic decision before us and it [was] its rationale that the government challenge[d]."[149] After reviewing the briefs of the government and two *amici curiae*, the American Civil Liberties Union (joined on the brief by the Center for Democracy and Technology, the Center for National Security Studies, the Electronic Privacy Information Center, and the Electronic Frontier Foundation) and the National Association of Criminal Defense Lawyers, the Court of Review concluded that "FISA, as amended by the Patriot Act, supports the government's position, and that

---

[145] *Id.* at 625.

[146] *Id.*

[147] *Id.* at 627.

[148] *Id.*

[149] In re Sealed Case, 310 F.3d 717, 721 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002) (hereinafter *Court of Review op.*).

the restrictions imposed by the FISA court are not required by FISA or the Constitution."[150]

Discussion of the Opinion. The Court of Review began its analysis by articulating its view of the May 17th FISC decision. The Court of Review stated that the FISC appeared to proceed in its opinion from the assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law enforcement officers in the Executive Branch, but did not support that assumption with any relevant language from the statute.[151] The Court of Review opined that this "wall" was implicit in the FISC's "apparent" belief that "it can approve applications for electronic surveillance only if the government's objective is *not* primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity," while referencing neither statutory language in FISA nor USA PATRIOT Act amendments, which the government argued altered FISA to permit an application even if criminal prosecution was the primary goal.[152] Instead, the Court of Review noted that the FISC relied upon its statutory authority with to approve "minimization procedures" in imposing the restrictions at issue.

The Court of Review stated that the government raised two main arguments: First, DOJ contended that the restriction, recognized by several courts of appeals [153]

---

[150] *Id.* at 719-20.

[151] *Id.* at 721.

[152] *Id.*

[153] The cases to which this appears to refer include decisions by both U.S. courts of appeals and U.S. district courts. Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, United States v. Megahey, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), *aff'd without opinion*, 729 F.2d 1444 (2d Cir. 1982), *re-aff'd post-trial sub nom* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987); United States. v Badia, 827 F. 2d 1458, 1464 (11th Cir. 1987). *See also*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), *rehearing and cert. denied*, 506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); United States v. Pelton, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S.1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard–i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense--for issuance of a search

(continued...)

[153] (...continued)
warrant was violative of the Fourth Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); United States v. Cavanaugh, 807 F.2d 787, 790-91 (9th Cir. 1987) (defendant, convicted of espionage, appealed district court's refusal to suppress fruits of FISA electronic surveillance which intercepted defendant offering to sell defense secrets to representatives of Soviet Union. In affirming conviction, appellate court found FISA procedures had been followed, and upheld FISA against constitutional challenges. Court found, in part, that FISA probable cause requirement was reasonable under Fourth Amendment standard. "The application must state that the target of the electronic surveillance is a foreign power or an agent of a foreign power, and must certify that the purpose of the surveillance is to obtain foreign intelligence information and that the information cannot reasonably be obtained by normal investigative techniques. 50 U.S.C. § 1804(a). It is true, as appellant points out in his brief, that the application need not state that the surveillance is likely to uncover evidence of a crime; but as the purpose of the surveillance is not to ferret out criminal activity but rather to gather intelligence, such a requirement would be illogical. *See United States District Court*, 407 U.S. at 322 (recognizing distinction between surveillance for national security purposes and surveillance of 'ordinary crime'); . . . And . . . there is no merit to the contention that he is entitled to suppression simply because evidence of his criminal conduct was discovered incidentally as the result of an intelligence surveillance not supported by probable cause of criminal activity. *See Duggan*, 743 F.2d at 73n.5.") United States v. Rahman, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). *Cf.*, United States v. Bin Laden, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); United States v. Bin Laden, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection. . . . If foreign intelligence collection is merely *a* purpose and not the *primary* purpose of a search, the exception does not apply.")

Cf., United States v. Sarkissian, 841 F.2d 959, 964-65 (9th Cir. 1988) (FISA court order authorized electronic surveillance, which resulted in the discovery of plan to bomb the Honorary Turkish Consulate in Philadelphia, and of the fact that bomb components were being transported by plane from Los Angeles. The FBI identified likely airlines, flight plans, anticipated time of arrival, and suspected courier. Shortly before the arrival of a flight fitting these parameters, the investigation focused upon an individual anticipated to be a passenger on that flight. An undercover police officer spotted a man matching the suspected courier's description on that flight. The luggage from that flight was sniffed by a trained dog and x-rayed. A warrantless search was conducted of a suitcase that had been shown by x-ray to contain an unassembled bomb. Defendants unsuccessfully moved to suppress the evidence from the FISA wiretap and the warrantless search. On appeal the court upheld the warrantless suitcase search as supported by exigent circumstances. Defendants contended that the FBI's primary purpose for the surveillance had shifted at the time of the wiretap from an intelligence investigation to a criminal investigation and that court approval for the wiretap therefore should have been sought under Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*, rather than FISA. The court, while noting that in other cases it had state that "the purpose of [electronic] surveillance" under FISA "must be to secure foreign intelligence information," "not to ferret out criminal activity;" declined to decide the issue of whether the applicable standard was that "the purpose" or that "the primary purpose" of a FISA surveillance must be gathering of foreign intelligence information. The court stated, "Regardless of whether the test is one of purpose or primary purpose, our review of the government's FISA materials convinces

(continued...)

prior to the enactment of the USA PATRIOT Act, that FISA could only be used if the government's primary purpose in gathering foreign intelligence information was not criminal prosecution was not supported by the statutory language or the legislative history of FISA. This argument was not presented to the FISC, but the Court of Review indicated that it could entertain this argument, because proceedings before the FISC and before the Court of Review were *ex parte*.[154] Second, the government argued that, even if the primary purpose test was appropriate prior to the passage of the USA PATRIOT Act, the amendments made by that act eliminated that concept. The government also argued that the FISC's interpretation of the minimization procedures provisions misconstrued those provisions and amounted to "an end run" around the USA PATRIOT Act amendments. DOJ argued further that the FISC minimization procedures so intruded into the Department's operations as to be beyond the constitutional authority of Article III judges. Finally, DOJ contended that application of the primary purpose test in a FISA case was not constitutionally compelled under the Fourth Amendment.

---

[153] (...continued)
us that it is met in this case. . . . We refuse to draw too fine a distinction between criminal and intelligence investigations. "International terrorism ," by definition, requires the investigation of activities that constitute crimes. 50 U.S.C. § 1806(f). That the government may later choose to prosecute is irrelevant. FISA contemplates prosecution based on evidence gathered through surveillance. . . . "Surveillances . . . need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate." S. Rep. No. 701, 95th Cong., 1st Sess. 11 . . . .[(1978)]. . . .FISA is meant to take into account "the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities . . ." *Id.* . . . . At no point was this case an ordinary criminal investigation."). *Cf.*, United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) (distinguishing United States v. Truong Dinh Hung, 629 F.2d 908, 912-13 (4th Cir. 1980); and United States v. Butenko, 494 F.d 593, 606 (3d Cir.) (*en banc*), *cert. denied sub nom*, Ivanov v. United States, 419 U.S. 881 (1974), which held that, while warrantless electronic surveillance for foreign intelligence purposes was permissible, when the purpose or primary purpose of the surveillance is to obtain evidence of criminal activity, evidence obtained by warrantless electronic surveillance is inadmissible at trial, 540 F. Supp. at 1313; on the theory that the evidence in the case before it was obtained pursuant to a warrant–a lawfully obtained court order under FISA, *id.* at 1314. The court noted that the "bottom line of *Truong* is that evidence derived from *warrantless* foreign intelligence searches will be admissible in a criminal proceeding only so long as the primary purpose of the surveillance is to obtain foreign intelligence information." *Id.* at 1313-14. After noting that Congress, in enacting FISA, "expected that evidence derived from FISA surveillances could then be used in a criminal proceeding," the court concluded that "it was proper for the FISA judge to issue the order in this case because of the on-going nature of the foreign intelligence investigation. . . . The fact that evidence of criminal activity was thereafter uncovered during the investigation does not render the evidence inadmissible. There is no question in [the court's] mind that the purpose of the surveillance, pursuant to the order, was the acquisition of foreign intelligence information. Accordingly, [the court found] that the FISA procedures on their face satisfy the Fourth Amendment warrant requirement, and that FISA was properly implemented in this case." *Id.* at 1314.).

[154] *Court of Review op.*, 310 F.3d at 722 n.6.

The Court of Review noted that, as enacted in 1978, FISA authorized the grant of an application for electronic surveillance to obtain foreign intelligence information if there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power,"[155] and that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power."[156] The reviewing court focused upon the close connection between criminal activity and the definitions of "agent of a foreign power" applicable to United States persons contained in 50 U.S.C. §§ 1801(b)(2)(A) and (C), to wit: "any person who 'knowingly engages in clandestine intelligence activities . . . which activities involve or may involve a violation of the *criminal statutes* of the United States,' or 'knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor.'"[157] The court noted further that FISA defined "international terrorism" to mean "activities that 'involve violent acts or acts dangerous to human life that are a violation of the *criminal laws* of the United States or of any State, or that would be a *criminal*

---

[155] The Court of Review did not include in its quotation of 50 U.S.C. § 1805(a)(3)(A) the proviso that follows the quoted language: "*Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."

[156] *Court of Review op.*, 310 F.3d at 722, *quoting* portions of 50 U.S.C. § 1805(a)(3).

[157] *Id.* at 723 (emphasis added by the Court of Review). The definitions of "agent of a foreign power" which apply to "any person" (including, by implication, United States persons) are set forth in 50 U.S.C. § 1801(b)(2). This subsection now contains five subparagraphs:

> (b) "Agent of a foreign power" means–
>
> . . .
>
> (2) any person who–
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power, or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

The current subparagraph (D) was added in 1999, and the former subparagraph (D) was redesignated subparagraph (E).

violation if committed within the jurisdiction of the United States or any State.'"[158] "Sabotage," as defined by FISA, covers activities that "'involve a violation of chapter 105 of [the criminal code] [18 U.S.C. §§ 2151-2156], or that would involve such a violation if committed against the United States.'"[159] For purposes of its opinion, the Court of Review described these types of crimes as "foreign intelligence crimes."[160]

---

[158] *Id.* at 723, *quoting* 50 U.S.C. § 1801(c)(1) (emphasis added by the Court of Review). The remainder of the definition of "international terrorism" under 50 U.S.C. § 1801(c)(2) and (3) adds two more criteria for activities to be considered to be within this definition:

> (c) "International terrorism" means activities that–
>
> . . .
>
> (2) appear to be intended–
>
> (A) to intimidate or coerce a civilian population;
>
> (B) to influence the policy of a government by intimidation or coercion; or
>
> (C) to affect the conduct of a government by assassination or kidnapping; and
>
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

[159] *Court of Review slip op.* at 10, quoting 50 U.S.C. § 1801(d).

[160] Although later acknowledging the possibility that the Justice Department had accepted the dichotomy between foreign intelligence gathering and law enforcement purposes "in an effort to conform to district court holdings," *Court of Review op.*, 310 F.3d at 727, (most of the published decisions were court of appeals decisions rather than district court decisions) the Court of Review expressed puzzlement that "the Justice Department, at some point during the 1980's, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents–even for foreign intelligence crimes," while noting that 50 U.S.C. § 1804 at the time required that "a national security official in the Executive Branch–typically the Director of the FBI– . . . certify that 'the purpose' of the surveillance was to obtain foreign intelligence information (amended by the Patriot Act to read 'a significant purpose.')" *Id.* at 723. The court did, however, discuss a series of 1982-1991 cases upholding the constitutional sufficiency of electronic surveillance under FISA as long as "the primary purpose" of the surveillance was gathering foreign intelligence information, rather than criminal prosecution. If foreign intelligence gathering was the primary purpose of a FISA electronic surveillance, initially and throughout the surveillance, and FISA was not being used as "an end run around the 4th Amendment," the courts permitted use of the fruits of the surveillance in subsequent criminal prosecutions. See the discussion of these cases at fn. 153, *supra*, of this report. This "primary purpose" approach to these FISA cases appears consistent with the "primary purpose" approach taken in a number of pre-FISA cases involving Fourth Amendment challenges to warrantless foreign intelligence surveillances. See constitutional analyses in United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (5th Cir. 1974); United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974) , *cert. denied sub nom*, Ivanov v. United States, 419 U.S. 881 (1974), and Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976); along with the Supreme Court's analysis, in a domestic surveillance context, in the *Keith* case, United States v. United States District Court, 407 U.S. 297 (1972), discussed in the "Background" section of this report, *supra*. The Court of Review appears to discount the significance of these decisions because the courts involved upheld

(continued...)

The court observed that, as passed in 1978, 50 U.S.C. §1804 required a national security official of the Executive Branch, usually the FBI Director,[161] to certify that "the purpose" of the electronic surveillance under FISA was to obtain foreign intelligence information, and opined that "it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power–if he or she is a U.S. person–is grounded on criminal conduct."[162] It found further support for its view that "foreign intelligence information" included evidence of "foreign intelligence crimes" from the legislative history as reflected in H.Rept. 95-1283 and S. Rept. 95-701, [163] while acknowledging that the House report also stated that FISA surveillances "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns

---

[160] (...continued)
lower court decisions permitting admission of information gathered under FISA in criminal trials. The Court of Review stated, "It may well be that the government itself, in an effort to conform to district court holdings, accepted the dichotomy it now contends is false. Be that as it may, since the cases that "adopt" the dichotomy do affirm district court opinions permitting the introduction of evidence gathered under a FISA order, there was not much need for the courts to focus on the opinion with which we are confronted." *Court of Review op.*, 310 F.3d at 727.

[161] The pertinent language of 50 U.S.C. § 1804(a)(7) as passed in 1978 provided that each application for an order authorizing electronic surveillance under FISA shall include:

> (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate–
>
> (A) that the certifying official deems the information sought to be foreign intelligence information;
>
> (B) that the purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
>
> (E) including a statement of the basis for the certification that–
>
> (i) the information sought is the typ0e of foreign intelligence information designated; and
>
> (ii) such information cannot reasonably be obtained by normal investigative techniques[.]

Under 50 U.S.C. § 1804(d) as passed in 1978 and under current law, "The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title."

[162] *Court of Review op.*, 310 F.3d at 723.

[163] *Id.* at 724-25, *citing* H.Rept. 95-1283, at 49 (1978) and S. Rept. 95-701, at 10-11 (1978).

United States persons must be necessary to important national concerns."[164] The Court of Review regarded the latter statement as an observation rather than a proscription.[165]

The Court of Review saw the U.S. Court of Appeals for the Fourth Circuit's decision in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), a decision based upon constitutional analysis rather than FISA provisions, as the springboard for the "primary purpose" test cases interpreting FISA and upholding FISA surveillances against Fourth Amendment challenges.[166] After reviewing a number of the FISA cases applying the primary purpose test, the Court of Review concluded that a dichotomy between foreign intelligence gathering and criminal investigations implicit in the application of the primary purpose test was not statutorily compelled. The court found that FISA, as originally passed, did not "preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."[167] In addition, the Court of Review, relying on arguments of the Department of Justice and the language of subsection 1805(a)(5), interpreted 50 U.S.C. §§ 1805 of FISA as originally enacted as not contemplating that the [FISC] would inquire into the government's purpose in seeking foreign intelligence information.[168]

---

[164] H.Rept. 95-1283, at 36 (1978).

[165] *Court of Review op.*, 310 F.3d at 725.

[166] Although *Truong Dinh Hung* was among the cases cited by some of the subsequent FISA cases, a "primary purpose" test had been previously applied in the 1974 Third Circuit decision in *Butenko, supra,* upholding a warrantless electronic surveillance in the face of challenges based upon the Fourth Amendment and Section 605 of the Communications Act where the primary purpose of the investigation was gathering foreign intelligence information. See discussion in the "Background" section of this report, *supra*, as well as the summary of this and other cases at fns. 153 and 160, *supra.*

[167] *Court of Review op.*, 310 F.3d at 727.

[168] *Id.* at 723-24, 728. Section 1805(a), as enacted in 1978, set forth the necessary findings that a judge of the FISC had to make in order to enter an ex parte order as requested or as modified approving electronic surveillance under FISA:

> (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
> (2) the application has been made by a Federal officer and approved by the Attorney General;
> (3) on the basis of the facts submitted by the applicant there is probable cause to believe that–
> (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
> (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(continued...)

Further, the court rejected the FISC's characterization of the Attorney General's 1995 procedures, as modified and augmented in January 2000 and August 2001, as minimization procedures. These procedures were formally adopted by the FISC as minimization procedures defined in 50 U.S.C. §§ 1801(h) and 1821(4) in November 2001, after passage of the USA PATRIOT Act, and were incorporated in all applicable orders and warrants granted since their adoption by the FISC. On March 6, 2002, the Attorney General adopted new "Intelligence Sharing Procedures," intended to supercede prior procedures, to "allow complete exchange of information and advice between intelligence and law enforcement officials," to "eliminate the 'direction and control' test," and to permit "exchange of advice between the FBI, OIPR, and the Criminal Division regarding 'the initiation, operation, continuation, or expansion of FISA searches or surveillance."[169] The following day, the government filed a motion with the FISC advising the court of the Attorney General's adoption of the 2002 procedures, seeking to have that court adopt the new procedures in all matters before the FISC and asking the court to vacate its orders adopting the prior procedures as minimization procedures and imposing "wall" procedures in certain types of cases. That motion led to the FISC decision to adopt the 2002 procedures with modifications that was, by reference, before the Court of Review in its November 18, 2002, decision.

The Court of Review characterized the FISC's adoption of the Justice Department's 1995 procedures, as modified and augmented, as minimization procedures as follows:

> Essentially, the FISA court took portions of the Attorney General's augmented 1995 Procedures--adopted to deal with the primary purpose standard–and imposed them generically as minimization procedures. In doing so, the FISA court erred. It did not provide any constitutional basis for its action–we think there is none–and misconstrued the main statutory provision on which it relied. The court mistakenly categorized the augmented 1995 Procedures as FISA minimization procedures and then compelled the government to utilize a modified version of those procedures in a way that is clearly inconsistent with the statutory purpose.[170]

The Court of Review interpreted "minimization procedures" under 50 U.S.C. § 1801(h) to be designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information which is not foreign intelligence information. In light of the Court of Review's interpretation of "minimization procedures" under 50 U.S.C. § 1801(h), the court found no basis for

---

[168] (...continued)

> (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title;
>
> (5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

[169] *Court of Review op.*, 310 F.3d at 729.

[170] *Id.* at 730.

the FISC's reliance upon that section "to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of a foreign intelligence crime."[171]

In addition, the Court of Review found that the FISC had misconstrued its authority under 50 U.S.C. § 1805 and misinterpreted the definition of minimization procedures under 50 U.S.C. § 1801(h). The Court of Review expressed approbation for the Government's argument that the FISC, in imposing the modified 1995 procedures upon the Department of Justice as minimization procedures, "may well have exceeded the constitutional bounds that restrict an Article III court. The FISA court asserted authority to govern the internal organization and investigative procedures of the Department of Justice which are the province of the Executive Branch (Article II) and the Congress (Article I)."[172]

The Court of Review deemed the FISC's "refusal . . . to consider the legal significance of the Patriot Act's crucial amendments [to be] error."[173] The appellate court noted that, as amended by the USA PATRIOT Act, the requirement in 50 U.S.C. § 1804(a)(7)(B) that the Executive Branch officer certify that "the purpose" of the FISA surveillance or physical search was to gather foreign intelligence information had been changed to "a significant purpose."[174] The court noted that floor statements indicated that this would break down traditional barriers between law enforcement and foreign intelligence gathering,[175] making it easier for law enforcement to obtain FISA court orders for surveillance or physical searches where the subject of the surveillance "is both a potential source of valuable intelligence and the potential target of a criminal prosecution."[176] The court noted that some Members raised concerns about the Fourth Amendment implications of this language change which permitted the Government to obtain a court order under FISA "even if the

---

[171] *Id.* at 731.

[172] *Id.* at 731-32.

[173] *Id.* at 732.

[174] *Id.* at 728-29, 732-33.

[175] *Id.* at 732, *quoting* Sen. Leahy, 147 Cong. Rec. S10992 (Oct. 25, 2001).

[176] *Id.* at 733, *quoting* Sen. Feinstein, 147 Cong. Rec. S10591 (Oct. 11, 2001). In Section 13.5 of Chapter 13 of its *Final Report*, at 424, the 9/11 Commission, in discussing the future role of the FBI, observes in part:

> Counterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action. Because the FBI can have agents working criminal matters and agents working intelligence investigations concerning the same international terrorism target, the full range of investigative tools against a suspected terrorist can be considered within one agency. The removal of the "wall" that existed before 9/11 between intelligence and law enforcement has opened up new opportunities for cooperative action within the FBI.

primary purpose is a criminal investigation."[177] Interestingly, although the Court of Review did not regard a dichotomy between foreign intelligence gathering and law enforcement purposes as necessarily implied by the 1978 version of 50 U.S.C. § 1804(a)(7)(B), the court viewed the statutory change from "the purpose" to "a significant purpose" in the USA PATRIOT Act as recognizing such a dichotomy.[178]

The Court of Review disagreed with the FISC interpretation of the consultation authority under 50 U.S.C. § 1806(k).[179] The Court of Review saw this provision as one which reflected the elimination of barriers between law enforcement and intelligence or counterintelligence gathering, without a limitation on law enforcement officers directing or controlling FISA surveillances. "[W]hen Congress explicitly authorizes consultation and coordination between different offices in the government, without even suggesting a limitation on who is to direct and control, it necessarily implies that either could take the lead."[180]

In analyzing the "significant purpose" amendment to 50 U.S.C. § 1804(a)(7)(B), the Court of Review deemed this a clear rejection of the primary purpose test. If gathering foreign intelligence information is a significant purpose, another purpose such as criminal prosecution could be primary.[181] Further, the court found that the term "significant" "imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes. . . . Although section 1805(a)(5) . . . may well have been intended to authorize the FISA court to review only the question whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804, it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information."[182] The Court of Review saw the "significant purpose" language as "excluding from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution."[183] If the government, at the commencement of a FISA surveillance has not yet determined whether to prosecute the target, "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test."[184] Under the Court of Review's analysis:

> If the certification of the application's purpose articulates a broader objective than criminal prosecution–such as stopping an ongoing conspiracy–and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was

---

[177] *Id.*, *quoting* Sen. Feingold, 147 Cong. Rec. S11021 (Oct. 25, 2001).

[178] *Id.* at 734-35.

[179] *Id.* at 733-34.

[180] *Id.* at 734.

[181] *Id.* at 734.

[182] *Id.* at 735.

[183] *Id.*

[184] *Id.*

> merely to gain evidence of past criminal conduct–even foreign intelligence crimes–to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.[185]

The court stated further that, while ordinary crimes may be intertwined with foreign intelligence crimes, the FISA process may not be utilized to investigate wholly unrelated ordinary crimes.[186] The Court of Review emphasized that the government's purpose as reflected in the Section 1804(a)(7)(B) certification is to be judged by the FISC on the basis of

> . . .the national security officer's articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved. It is up to the Director of the FBI, who typically certifies, to determine the government's national security purpose, as approved by the Attorney General or Deputy Attorney General. . . . That means, perforce, if the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose–or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval. The important point is that the relevant purpose is that of those senior officials in the Executive Branch who have the responsibility of appraising the government's national security needs."[187]

Turning from its statutory analysis to its examination of whether the statute, as amended, satisfied Fourth Amendment parameters, the Court of Review compared the FISA procedures with those applicable to criminal investigations of "ordinary crimes" under Supreme Court jurisprudence and under the wiretap provisions of Title III of the Omnibus Crime Control and Safe Streets Act. Relying upon *Dalia v. United States*, 441 U.S. 238, 255 (1979), the court indicated that in criminal investigations, beyond requiring that searches and seizures be reasonable, the Supreme Court has interpreted the Fourth Amendment's warrant requirement to demand satisfaction of three criteria: a warrant must be issued by a neutral, detached magistrate; those seeking the warrant must demonstrate to the magistrate that there is probable cause to believe that the evidence sought will assist in a particular apprehension or conviction for a particular offense; and the warrant must describe with particularity the things to be seized and the place to be searched.[188]

The Court of Review compared the procedures in Title III with those in FISA, finding in some respects that Title III had higher standards, while in others FISA included additional safeguards. In both, there was provision for a detached, neutral magistrate. The probable cause standard in Title III for criminal investigations was deemed more demanding than that in FISA. Title III requires a showing of probable cause that a specific individual has committed, is committing, or is about to commit a particular criminal offense. FISA requires a showing of probable cause that the target of the FISA investigative technique is a foreign power or an agent of a foreign

---

[185] *Id.*

[186] *Id.* at 736.

[187] *Id.*

[188] *Id.* at 738.

power. A foreign power is not defined solely in terms of criminal activity. In the case of a target who is a U.S. person, the definition of "agent of a foreign power" contemplates, in part, the involvement of or, in the case of clandestine intelligence activities for a foreign power, the possibility of criminal conduct. The court regarded the lesser requirement with respect to criminal activity in the context of clandestine intelligence activities as to some extent balanced by the safeguard provided by FISA's requirement that there be probable cause to believe that the target is acting "for or on behalf of a foreign power."[189]

With regard to the particularity requirement, as to the first element, Title III requires a finding of probable cause to believe that the interception will obtain particular communications regarding a specified crime. In contrast, FISA requires an official to designate the type of foreign intelligence information being sought and to certify that the information being sought is foreign intelligence information. When the target of the FISA investigation is a U.S. person, the standard of review applied by the FISC is whether there is clear error in the certification, a lower standard that a judicial finding of probable cause. While the FISC can demand that the government provide further information needed for the court to make its determination as to whether the certification is clearly erroneous, the statute relies also upon internal checks on Executive Branch decisions through the requirement that the certification must be made by a national security officer and approved by the Attorney General or Deputy Attorney General.

In connection with the second particularity element, Title III

> . . . requires probable cause to believe that the facilities subject to surveillance are being used or are about to be used in connection with commission of a crime or are leased to, listed in the name of, or used by the individual committing the crime, 18 U.S.C. § 2518(3)(d), [while] FISA requires probable cause to believe that each of the facilities or places at which the surveillance is directed is being used, or is about to be used by a foreign power or agent [of a foreign power]. 50 U.S.C. § 1805(a)(3)(B). . . . Simply put, FISA requires less of a nexus between the facility and the pertinent communications that Title III, but more of a nexus between the target and the pertinent communications."[190]

The Court of Review also compared Title III to FISA with respect to necessity (both statutes require that the information sought is not available through normal investigative procedures, although the standards differ somewhat),[191] duration of

---

[189] *Id.* at 738-39.

[190] *Id.* at 740.

[191] For electronic surveillance to be approved, Title III requires a judicial finding that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. 18 U.S.C. § 2518(3)(c). FISA requires certification by the national security officer involved that the foreign intelligence information sought cannot reasonably be obtained by normal investigative means. 50 U.S.C. § 1804(a)(7)(C). The certification must include a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated; and that such information cannot reasonably be obtained by normal investigative techniques.

(continued...)

surveillance (30 days under Title III, 18 U.S.C. § 2518(3)(c), as opposed to 90 days under FISA for U.S. persons, 50 U.S.C. § 1805(e)(1)),[192] minimization and notice.

With respect to minimization, the Court of Review noted that Title III, under 18 U.S.C. § 2518(5), required minimization of what was acquired, directing that surveillance be carried out "in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." FISA, on the other hand, "requires minimization of what is acquired, retained, and disseminated."[193] Observing that the FISC had found "in practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications," the Court of Review deemed the reasonableness of such an approach to be dependent upon the facts and circumstances of each case:[194]

> Less minimization in the acquisition stage may well be justified to the extent the intercepted communications are "ambiguous in nature or apparently involve[] guarded or coded language," or "the investigation is focusing on what is thought to be a widespread conspiracy [where] more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise." . . . Given the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots. . . .[195]

With respect to notice, the Court of Review observed that under 18 U.S.C. § 2518(8)(d), Title III mandated notice to the target of the surveillance and, in the judge's discretion, to other persons whose communications were intercepted, after the surveillance has expired. In contrast, under 50 U.S.C. § 1806(c) and (d), FISA does not require notice to a person whose communications were intercepted unless the government intends to use, disclose, or enter into evidence those communications or derivative information in a trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other federal, state or local authority against that person. The Court of Review noted that where such information was to

---

[191] (...continued)
50 U.S.C. § 1804(a)(7)(E)(i) and (ii). In issuing an ex parte order granting an application for electronic surveillance, the FISC judge must find that, in the case of a target who is a U.S. person, the certifications are not clearly erroneous on the basis of the statement made under 50 U.S.C. § 1804(a)(7)(e) and any other information furnished under Section 1804(d). Thus, the relevant findings to be made by the courts under the two statutes differ.

[192] *Court of Review op.*, 310 F.3d at 740. The difference, in the court's view, was "based on the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.' *Keith*, 407 U.S. at 322; *see also* S. Rep. at 16, 56." The court also noted that in FISA the "longer surveillance period is balanced by continuing FISA court oversight of minimization procedures during that period. 50 U.S.C. § 1805(e)(3); *see also* S Rep. at 56."

[193] *Id.*

[194] *Id.*

[195] *Id.* at 740-41.

be used against a criminal defendant, he or she would be given notice, and stated that "where such evidence is not ultimately going to be used for law enforcement," Congress had observed that "[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement."[196] In a footnote, the court noted that the Amici had drawn attention to the difference in the nature of the notice given the defendant or aggrieved person under Title III as opposed to FISA. Under Title III, a defendant is generally entitled under 18 U.S.C. § 2518(9) to obtain the application and order to challenge the legality of the surveillance. However, under FISA, the government must give the aggrieved person and the court or other authority (or in the case of a State or local use, the state or political subdivision must give notice to the aggrieved person, the court or other authority, and the Attorney General) of their intent to so disclose or use communications obtained from the surveillance or derivative information. In addition, under 50 U.S.C. §§ 1806(f) and (g), if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm national security, the U.S. district court may review in camera and ex parte the application, order, and other materials related to the surveillance, to determine whether the surveillance was lawfully authorized and conducted, whether disclosure or discovery is necessary, and whether to grant a motion to suppress. The Court of Review noted that these determinations are to be made by the U.S. District Judge on a case by case basis, and stated that "whether such a decision protects a defendant's constitutional rights in a given case is not before us."[197]

Based on this comparison of Title III and FISA, the Court of Review found that "to the extent that the two statutes diverge in constitutionally relevant areas– in particular, in their probable cause and particularity showings–a FISA order may not be a 'warrant' contemplated by the Fourth Amendment. . . . Ultimately, the question becomes whether FISA, as amended by the Patriot Act, is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens."[198]

The court framed the question as follows: "does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable." In its analysis, the court first considered whether the *Truong* case articulated the correct standard. *Truong* held that the President had inherent authority to conduct warrantless searches to obtain foreign intelligence information, but did not squarely address FISA. Starting from the perspective that *Truong* deemed the primary purpose test to be constitutionally compelled as an application of the *Keith* case balancing standard, the Court of Review found that the *Truong* determination that "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and . . . individual privacy interests come to the fore and government

---

[196] *Id.* at 741, *quoting* S.Rept. 95-701 at 12.

[197] *Id.*

[198] *Id.* at 741-42.

foreign policy concerns recede when the government is primarily attempting to form the basis of a criminal investigation."[199] The Court of Review found that this analysis was based upon a faulty premise that in the context of criminal prosecution "foreign policy concerns recede," and found further that the line the *Truong* court "sought to draw was inherently unstable, unrealistic, and confusing."[200] The Court of Review opined that in the context of counterintelligence, foreign policy concerns did not recede when the government moved to prosecute. Rather "the government's primary purpose is to halt the espionage or terrorism efforts, and criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts."[201]

In addition, the court found that the method of determining when an investigation became primarily criminal by looking to when the Criminal Division of the Department of Justice assumed the lead role, had led over time to the "quite intrusive organizational and personnel tasking the FISA court [had] adopted."[202] The court found the "wall" procedure to generate dangerous confusion and create perverse organizational incentives that discouraged wholehearted cooperation of "all the government's personnel who can be brought to the task."[203] This the court suggested could be thought to be dangerous to national security and could be thought to discourage desirable initiatives.

In addition, the court saw the primary purpose test as administered by the FISC, "by focusing on the subjective motivation of those who initiate investigations . . . was at odds with the Supreme Court's Fourth Amendment cases which regard subjective motivation of an officer conducting a search or seizure as irrelevant." [204]

Assuming *arguendo* that FISA orders were not warrants within the scope of the Fourth Amendment, the Court of Review returned to the question of whether searches under FISA are constitutionally reasonable. While the Supreme Court has not considered directly the constitutionality of warrantless government searches for foreign intelligence purposes, the balance between the government's interest and personal privacy interests is key to an examination of this question. The Court of

---

[199] *Id.* at 742-43, *citing Truong*, *supra*, 629 F.2d at 914-15.

[200] *Id.* at 743.

[201] *Id.*

[202] *Id.*

[203] *Id.*

[204] *Id.*, *citing* Whren v. United States, 517 U.S. 806, 13 (1996). *See also*, Arkansas v. Sullivan, 532 U.S. 769, 770-72 (2001); Scott v. United States, 438 U.S. 128, 135-138 (1978). In these cases, the Court has held that in a Fourth Amendment probable cause analysis of a warrantless search or seizure, the fact that an otherwise lawful search or seizure may have been made as a pretext for searching for evidence of other criminal behavior does not render that search or seizure unconstitutional. One might note that the probable cause standard applicable to a search or seizure in a criminal investigation is different from that under FISA, so that the pretextual search criminal cases may not be directly analogous to the FISA situation.

Review viewed *Keith* as suggesting that a somewhat relaxed standard might be appropriate in foreign intelligence crimes as opposed to ordinary crimes.[205]

The Court of Review then briefly touched upon the Supreme Court's "special needs" cases, where the Court upheld searches not based on a warrant or individualized suspicion in extraordinary circumstances involving "special needs, beyond the normal need for law enforcement." In *City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000), the U.S. Supreme Court held that a highway check point program designed to catch drug dealers was not within the "special needs" exception to the requirement that a search be based upon individualized suspicion, because "the government's 'primary purpose' was merely 'to uncover evidence of ordinary criminal wrongdoing.'" The Court stated that "the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose."[206] The Court relied upon an examination of the primary purpose of the program, but not the motivations of individual officers, to determine whether the "special needs" standard had been met. The Supreme Court noted that an appropriately tailored road block could be used "to thwart an imminent terrorist attack."[207]

After summarizing *Edmond*, the Court of Review emphasized that it is the nature of the threat or emergency that took the matter beyond the realm of ordinary crime control.[208] It concluded that, while the gravity of the threat alone cannot be dispositive of the reasonableness of a search under the Fourth Amendment standard, it is a critical factor in the analysis. In its view, the "programmatic purpose" of FISA, "to protect the nation against terrorists and espionage threats directed by foreign powers," was one which, from FISA's inception, was distinguishable from "ordinary crime control."[209] The Court of Review also concluded that, "[e]ven without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close."[210] Applying the balancing test that it had drawn from *Keith* between foreign intelligence crimes and ordinary crimes, the Court of Review held surveillances under FISA, as amended by the USA PATRIOT Act, were reasonable and therefore constitutional. In so doing, however, the Court of Review

> acknowledge[d] . . . that the constitutional question presented by this case–whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment–has no definitive jurisprudential answer. The Supreme Court's special needs cases involve random stops (seizures) not electronic searches. In one sense, they can be thought of as a greater encroachment into personal privacy because they are not based on any particular

---

[205] *Id.* at 744.

[206] 531 U.S. at 42, *cited in Court of Review op.*, 310 F.3d at 745.

[207] 531 U.S. at 44, *cited in Court of Review op.*, 310 F.3d at 746.

[208] *Court of Review op.*, 301 F.3d at 746.

[209] *Id.*

[210] *Id.*

> suspicion. On the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning.[211]

The Court of Review reversed the FISC's orders before it for electronic surveillance "to the extent they imposed conditions on the grant of the government's applications, vacate[d] the FISA court's Rule 11, and remand[ed] with instructions to grant the applications as submitted and proceed henceforth in accordance with this opinion."[212]

50 U.S.C. § 1803(b) provides that, where the Court of Review upholds a denial by the FISC of a FISA application, the United States may file a petition for certiorari to the United States Supreme Court. Since consideration of applications for FISA orders is ex parte, there is no provision in FISA for an appeal to the United States Supreme Court from a decision of the Court of Review by anyone other than the United States. Nevertheless, on February 18, 2003, a petition for leave to intervene and a petition for writ of certiorari to the U.S. Foreign Intelligence Surveillance Court of Review was filed in this case in the U.S. Supreme Court by the American Civil Liberties Union, National Association of Criminal Defense Lawyers, American-Arab Anti-Discrimination Committee, and the Arab Community Center for Economic and Social Services. On March 14, 2003, the Bar Association of San Francisco filed a motion to file an amicus curiae brief in support of the motion to intervene and petition for certiorari. On March 24, 2003, the Supreme Court denied the motion for leave to intervene in order to file a petition for a writ of certiorari and denied the motion for leave to file an amicus curiae brief.[213]

Conclusion

The Foreign Intelligence Surveillance Act, as amended, provides a statutory structure to be followed where electronic surveillance, 50 U.S.C. § 1801 *et seq.*, physical searches, 50 U.S.C. § 1821 *et seq.*, or pen registers or trap and trace devices, 50 U.S.C. § 1841 *et seq.*, for foreign intelligence gathering purposes are contemplated. In addition, it provides a statutory mechanism for the FBI to seek production of "any tangible things" for an investigation seeking foreign intelligence information not involving a U.S. person or to protect against international terrorism or clandestine intelligence with respect to any person under the new version of 50 U.S.C. § 1861. FISA creates enhanced procedural protections where a United States person is involved, while setting somewhat less stringent standards where the surveillance involves foreign powers or agents of foreign powers. With its detailed statutory structure, it appears intended to protect personal liberties safeguarded by the

---

[211] *Id.*

[212] *Id.*

[213] American Civil Liberties Union v. United States, Docket No. 02M69, 538 U.S. ___ (March 24, 2003). The disposition of the case appears on the Supreme Court's Order List for that date. It is interesting to note that both the Petition for Leave to Intervene and Petition for a Writ of Certiorari filed by the American Civil Liberties Union, et al., and the motion to file an amicus curiae brief of the Bar Association of San Francisco were filed under the name In re: Sealed Case of the Foreign Intelligence Surveillance Court of Review No. 02-001.

First and Fourth Amendments while providing a means to ensure national security interests.

The USA PATRIOT Act, P.L. 107-56, increased the number of FISC judges from 7 to 11, while expanding the availability of FISA electronic surveillance, physical searches and pen registers and trap and trace devices. For example, under P.L. 107-56, an application for a court order permitting electronic surveillance or a physical search under FISA is now permissible where "a significant" purpose of the surveillance or physical search, rather than "the" purpose or, as interpreted by some courts, the primary purpose of the surveillance is to gather foreign intelligence information. While the previous language withstood constitutional challenge, the Supreme Court has not yet determined the constitutional sufficiency of the change in the FISA procedures under the Fourth Amendment.

The USA PATRIOT Act also amended FISA to allow court orders permitting so-called multipoint or "roving" electronic surveillance, where the orders do not require particularity with respect to the identification of the instrument, place, or facility to be intercepted, upon a finding by the court that the actions of the target of the surveillance are likely to thwart such identification. P.L. 107-108 further clarified this authority.

Under the act, pen registers and trap and trace devices may now be authorized for e-mails as well as telephone conversations. In addition, the act expanded the previous FBI access to business records, permitting court ordered access in connection with a foreign intelligence or international terrorism investigation not just to business records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities, but to any tangible things.

While expanding the authorities available for foreign intelligence investigations, FISA, as amended by the USA PATRIOT Act and the Intelligence Authorization Act for FY2002, also contains broader protections for those who may be the target of the various investigative techniques involved. For example, whether the circumstances involve electronic surveillance, physical searches, pen registers or trap and trace devices or access to business records and other tangible items, FISA, as amended by the USA PATRIOT Act, does not permit the court to grant orders based solely upon a United States person's exercise of First Amendment rights.[214]

In addition, P.L. 107-56 created a new private right of action for persons aggrieved by inappropriate disclosure or use of information gleaned or derived from electronic surveillance, physical searches or the use of pen registers or trap and trace devices. These claims can be brought against the United States for certain willful violations by government personnel.

Finally, the inclusion of a sunset provision for the FISA changes made in the USA PATRIOT Act, with the exception of the increase in the number of FISC judges,

---

[214] *See, e.g.*, 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A), 1842(a)(1), 1843(b), 1861(a)(1), and 1861(a)(2).

provides an opportunity for the new authorities to be utilized and considered, and an opportunity for the Congress to revisit them in light of that experience.[215]

Sections 898 and 899 of the Homeland Security Act of 2002, P.L. 107-296, amended FISA, 50 U.S.C. §§1806(k)(1) and 1825(k)(1) respectively, to permit federal officers conducting electronic surveillance or physical searches to acquire foreign intelligence information under FISA to consult with federal law enforcement officers "or law enforcement personnel of a state or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision)." Such consultations are to coordinate efforts to investigate or protect against actual or potential attacks or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage or international terrorism by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or an agent of a foreign power. These sections also state that such consultations do not preclude the Assistant to the President for National Security Affairs or other designated executive branch officials from making the necessary certifications as part of the application process for a FISA court order under 50 U.S.C. §§ 1804(a)(7) or 1823(a)(7), nor are these consultations to preclude entry of an order under 50 U.S.C. §§ 1805 or 1824.[216]

---

[215] Section 1503 of S. 22,108th Congress, as introduced, would amend Section 224(a) of the USA PATRIOT Act, P.L. 107-56, to insert "before the period the following: 'and any provision of law amended or modified by this title and the amendments made under this title (except for the sections excepted) shall take effect January 1, 2006, as in effect on the day before the effective date of this act.'" The effect of this language would be to eliminate the sunset provision for the FISA provisions from P.L. 107-56, as amended, and all other provisions subject to the Section 224(a) sunset provision. The sunset provision as originally enacted by P.L. 107-56 by its terms applies to all but a specific list of designated provisions and takes effect on December 31, 2005.

[216] Section 897 of the Homeland Security Act of 2002, which dealt with "Foreign Intelligence Information," amended Section 203(d)(1) of the USA PATRIOT Act to provide authority, consistent with the responsibility of the DCI to protect intelligence sources and methods and that of the Attorney General to protect sensitive law enforcement information,

> for information revealing a threat of an actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of an foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and the Director of Central Intelligence shall jointly issue.

(continued...)

Because historically the decisions of the FISC have not been made public, and because the opinion of the U.S. Foreign Intelligence Surveillance Court of Review discussed in this report was the first decision ever made by that court, the recent decisions of the FISC and the Court of Review provided a unique opportunity to observe the decision-making processes and differing perspectives of the two courts created by FISA.

The FISC's decision was set against a backdrop of a significant number of instances in which the Department of Justice had failed to maintain a "wall" between foreign intelligence gathering and criminal investigations. All seven of the then sitting members of the FISC concurred in the May 17th order of the court, written by the then presiding judge of the court. The FISC, in its May 17th opinion and order, treated the Attorney General's proposed 2002 "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI" as minimization procedures, and approved them as modified. The modifications made by the Court permitted the FBI, the Criminal Division, and OIPR to consult with one another "to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or their agents." In so doing, the FISC permitted such cooperation and coordination to address, among other things, the exchange of information already acquired, identification of categories of information needed and being sought, prevention of either foreign intelligence gathering or criminal law enforcement investigation or interest from obstructing or hindering the other; compromise of either investigation, and long term objectives and overall strategy of both investigations to insure that overlapping intelligence and criminal interests of the United States are both achieved.[217] While permitting direct consultation and coordination between components, the FISC required that OIPR be invited to all consultations and, if OIPR was unable to attend, the modified procedures required that OIPR be "forthwith" informed in writing of the substance of the meeting so that the FISC could be notified promptly.[218] In addition, under the procedures as modified by the FISC, law enforcement officials were prohibited from making recommendations to intelligence officials regarding the initiation, operation, continuation or expansion of FISA searches or surveillances. Nor could law enforcement officials direct or control the use of FISA procedures to enhance criminal prosecution. The FBI and the Criminal Division were given the responsibility to ensure that this did not occur, and were also required to make certain that advice intended to preserve the criminal prosecution option did not inadvertently result in the Criminal Division directing or controlling the investigation using FISA tools to

---

[216] (...continued)
In light of the Court of Review's interpretation of "foreign intelligence information" under FISA as including investigations of what the Court of Review termed "foreign intelligence crimes," it is not clear whether this section might be interpreted as applicable to sharing of information gleaned from FISA surveillances, searches, pen registers, trap and trace devices, or business record requests, particularly where criminal prosecution is a goal of the investigation.

[217] *FISC op.*, 218 F. Supp. 2d at 626.

[218] *Id.*

further law enforcement objectives.[219] In addition, the FISC adopted a new Rule 11, dealing with criminal investigations in FISA cases to monitor compliance with its May 17, 2002 order. This rule required all FISA applications to include informative descriptions of ongoing criminal investigations of FISA targets, as well as the substance of consultations between the FBI and criminal prosecutors at the Department of Justice or a U.S. Attorney's office.

In its November 18, 2002 opinion, the Court of Review took a starkly different view of the Attorney General's proposed procedures and firmly rejected the FISC analysis and conclusions. The issue came before the Court of Review as an appeal of two FISC orders, one granting an application to authorize electronic surveillance of an agent of a foreign power subject to restrictions stemming from the FISC May 17th opinion and order and the other renewing the authorization for electronic surveillance subject to the same conditions.

The Court of Review held that the FISC's interpretation of the augmented 1995 procedures and the proposed 2002 procedures as minimization procedures under 50 U.S.C. § 1801(h) was in error. The Court of Review found that the FISC had misconstrued 50 U.S.C. §§ 1801(h) and 1805 and may have overstepped its constitutional authority by asserting authority to govern the internal organization and investigative procedures of the Justice Department.

It found that FISA, as originally enacted, did not create a dichotomy between foreign intelligence information gathering and law enforcement investigations, nor did it require maintenance of a "wall" between such investigations. While FISA as enacted in 1978 required that a national security official certify that "the purpose" of the investigation was to gather foreign intelligence information, the court regarded the definition of "foreign intelligence information" as including evidence of criminal wrongdoing where a U.S. person is the target of the FISA investigation. In light of the fact that the definition of "agent of a foreign power" applicable to U.S. persons involved criminal conduct, or, in the context of clandestine intelligence operations, the possibility of criminal conduct, the court distinguished "foreign intelligence crimes" from "ordinary crimes." In foreign intelligence crimes, intelligence gathering and criminal investigations may become intertwined.

The Court of Review reviewed past court decisions requiring that, in seeking a FISA order authorizing electronic surveillance, the government must demonstrate that the "primary purpose" of the surveillance was to gather foreign intelligence information and not to further law enforcement purposes. Rejecting the "primary purpose test" as applied by the FISC and the courts of appeals of several circuits, the Court of Review did not find it to be compelled by the statutory language of FISA as enacted or by the Fourth Amendment.

The Court of Review also held the FISC to have been in error in its "refusal . . . to consider the legal significance of the Patriot Act's crucial amendments . . . ." In particular, the court focused upon the change of the required certification by the national security official from a certification that "the purpose" of the surveillance

---

[219] *Id.*

was to obtain foreign intelligence information to a certification that "a significant purpose" of the surveillance was to obtain foreign intelligence information in 50 U.S.C. § 1804(a)(7)(B); and the enactment of 50 U.S.C. § 1806(k), authorizing consultation and coordination by federal officers engaged in electronic surveillance to acquire foreign intelligence information with federal law enforcement officers.

Finding that the "significant purpose" amendment recognized the existence of a dichotomy between intelligence gathering and law enforcement purposes, the Court of Review concluded that this test was satisfied if the government had "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes."[220] While the gathering of foreign intelligence information for the sole objective of criminal prosecution would be precluded by the "significant purpose" language, if "the government entertains a realistic option of dealing with the agent [of a foreign power] other than through criminal prosecution," the court found the "significant purpose" test satisfied.[221] Although the court was of the view that, prior to passage of the USA PATRIOT Act, the FISC may well not have had authority under 50 U.S.C. § 1805(a)(5) to inquire into anything other than the issue of "whether the information sought was a type of foreign intelligence information, in light of the significant purpose amendment of section 1804" the Court of Review concluded that "it seems section 1805 must be interpreted as giving the FISA court the authority to review the government's purpose in seeking the information."[222] The court held that the government's purpose under 50 U.S.C. § 1804(a)(7)(B) was "to be judged by the national security official's articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved. . . . [I]f the FISA court has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose–or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval."[223]

The Court of Review also considered whether FISA, as amended, passed constitutional muster under the Fourth Amendment. It deemed the procedures and government showings required under FISA to come close to the minimum requirements for a warrant under the Fourth Amendment, if not meeting such requirements. Assuming *arguendo* that a FISA order was not a warrant for Fourth Amendment purposes, the Court of Review found FISA constitutional because the surveillances authorized thereunder were reasonable.

---

[220] *Id.* at 735.

[221] *Id.*

[222] *Id.*

[223] *Id.* at 736.

[redacted] (RMD) (FBI)

From: [redacted] (CTD) (FBI)
Sent: Friday, March 18, 2005 7:09 PM
To: [redacted] OGC)(FBI)
Cc: [redacted] (CTD) (FBI); [redacted] (CTD)(FBI)
Subject: CONUS 1 Patriot Act points

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Please see the attached from ITOS 1/CONUS 1
Thank you,

[redacted]

SSA [redacted]
CTD/ITOS 1/CONUS 1
Bldg: [redacted]
Room
Desk
Page

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179dmh/baw 05-cv-0845

[redacted] RMD) (FBI)

From: [redacted] (OGC)(FBI)
Sent: Thursday, March 17, 2005 1:01 PM
To: [redacted] (CTD) (FBI)
b6 **Cc:** [redacted] (OGC) (FBI); [redacted]
b7C (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: Follow-up Re Director's Senate Testimony

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

DATE: 12-13-2005 ALL INFORMATION CONTAINED
CLASSIFIED BY 65179dmh/baw 05-cv-0845 HEREIN IS UNCLASSIFIED EXCEPT
REASON: 1.4 (C) WHERE SHOWN OTHERWISE
DECLASSIFY ON: 12-13-2030

[redacted]

Here's some additional guidance beyond that which OCA offered (below).

Some examples of PATRIOT Act success that may prove helpful:

- **Sharing grand jury, Title III, and criminal investigative information.** [Sec. 203 was intended to eliminate barriers to timely sharing of information between criminal investigators and other entities (e.g., the IC, ICE, DoD, etc.) involved in the protection of national security. It gave the FBI full discretion to share criminal investigative information, regardless of its source, whenever it involves foreign intelligence information.]

b1 - **"Roving" FISA ELSUR authority.** [Sec. 206 was intended to counter a FISA target's
b2 attempts to use tradecraft to defeat ELSUR [redacted]
b7E [redacted] voiding the need to return to court for new secondary orders.] (S)
(S)

- **Changes in FISA PR/TT authority.** [Sec. 214 eliminated one of the showings that was previously required--i.e. [redacted] Now, the focus is simply on relevance to an investigation.]

b2
b7E

- **Changes in FISA business records authority.** [Sec. 215 assists the FBI in compelling production of business records. Previously, the FBI encountered situations in which holders of relevant records refused to produce them absent a subpoena or other compelling authority. Now, the FBI can seek a FISA court order for any such materials. Furthermore, the categories
b2 of things now attainable are much broader [redacted]
b7E [redacted]

- Also, if your folks happen upon any instances in which **library records** were obtained, that information would likewise be helpful.

Again, sincere thanks to you and your folks for all your help.

[redacted]

b6
b7C

-----Original Message-----
From [redacted] OGC)(FBI)
Sent: Thursday, March 17, 2005 11:33 AM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: Director's Senate Testimony

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

Request ITOS I help regarding the Director's testimony before the Senate Judiciary Committee on 5 April regarding the USA PATRIOT Act. (I stopped by your office this morning to discuss this. Sorry I missed you. I'll try again later.)

OCA is drafting the testimony. They've asked for our help in compiling **operational examples of USA PATRIOT Act successes**. Specifically, here's the guidance OCA provided:

b5

1. [redacted]
2.
3.
4.

[redacted]

OCA needs a draft of the testimony by Tuesday, 22 March. Given that deadline and all that needs to be accomplished in the interim, would it be possible to obtain the **ITOS I response by Friday afternoon, 18 March?** (Let me emphasize that we're not looking for every example--just an informal compilation of good examples that would assist the Director in driving home the Act's importance. And, as stated above, it's not important to be detailed or technical.)

Sincere thanks!

[redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SECRET

SECRET

[redacted]RMD) (FBI)

From: [redacted]OGC)(FBI)
Sent: Friday, March 18, 2005 11:05 AM
To: [redacted](CTD) (FBI)
Cc: [redacted](OGC) (FBI) [redacted](OGC) (FBI)
Subject: Follow-up Re PATRIOT Act Example

b6
b7C

DATE: 12-09-2005
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-09-2030

SECRET//ORCON,NOFORN
RECORD 66F-HQ-A1419826-z

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]--

Here's how I recommend revising your attached:

[redacted](S)

b1
b2
b7E
b5

Now, having said that, I'm not so sure we should offer this case as an example. As I understand its facts, the subject made extensive use of the cell phone[redacted]

[redacted]

Thanks again!

[redacted]

-----Original Message-----
From [redacted]CTD) (FBI)
Sent: Friday, March 18, 2005 9:58 AM
To [redacted]OGC)(FBI)
Subject: Take a look

b6
b7C

SECRET//ORCON,NOFORN
RECORD 66F-HQ-A1419826-z

b1
b2
b7E

[redacted]

Here is the example I wrote for Section 214.

(S//OC/NF) [redacted](S)

10/25/2005

(S)

b1
b2
b7E

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20300318
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20300318
SECRET//ORCON,NOFORN

[redacted] (RMD) (FBI)

From: [redacted] (OGC)(FBI)
Sent: Tuesday, March 22, 2005 5:11 PM
To: [redacted] OGC) (FBI)
Subject: FW: Bullets for Director's Senate Testimony

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

-----Original Message-----
From [redacted] (CTD) (FBI)
Sent: Friday, March 18, 2005 7:18 PM
To [redacted] TD) (FBI)
Cc [redacted] (OGC)(FBI)
Subject: FW: Bullets for Director's Senate Testimony

DATE: 12-13-2005
CLASSIFIED BY 65179DMH/BAW 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-13-2030

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Patriot Act tasking

[redacted]
Unit Chief
CTD/ITOS 1/Conus IV
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] CTD) (FBI)
Sent: Friday, March 18, 2005 11:01 AM
To [redacted] (CTD) (FBI)
Cc: [redacted] (CTD) (FBI); [redacted] (CTD) (FBI); [redacted] CTD) (FBI)
Subject: Bullets for Director's Senate Testimony

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]
Here is a bullet for the [redacted] division:

(U) In September 2004, a reliable source advised FBI that a subject of a Full Investigation had identified certain landmarks he/she wanted to attack. In addition to FISA ELSUR authority, FBI requested and received approval for mobile (roving) audio surveillance. While FBI received "roving" authority, technical issues did not allow FBI to utilize "roving" surveillanc[redacted] (S)

b1
b6
b7C

Thanks
[redacted]

SECRET

IA
CTD/ITOS I/CONUS IV

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SECRET

[redacted]RMD) (FBI)

From: [redacted](OGC)(FBI) b6
Sent: Tuesday, March 22, 2005 5:11 PM b7C
To: [redacted](OGC) (FBI)
Subject: FW: CONUS 1 Patriot Act points

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179dmh/baw 05-cv-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted](CTD) (FBI) b6
Sent: Friday, March 18, 2005 7:09 PM b7C
To: [redacted]OGC)(FBI)
Cc: [redacted](CTD) (FBI) [redacted]TD)(FBI)
Subject: CONUS 1 Patriot Act points

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Please see the attached from ITOS 1/CONUS 1
Thank you, b6 b7C
[redacted]

SSA [redacted]
CTD/ITOS 1/CONUS 1
[redacted] b2 b6 b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted](RMD) (FBI)

From: [redacted]OGC) (FBI)
Sent: Thursday, March 17, 2005 9:27 AM
To: [redacted]OGC)(FBI)
Subject: FW: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179dmh/baw 05-cv-0845

More on same subject that I just sent to you.
-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Thursday, March 17, 2005 7:26 AM
To: [redacted]OGC) (FBI); [redacted]. (OGC) (FBI) [redacted]OGC) (FBI); [redacted]OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

Could you get operaitonal examples for [redacted]or this project which we are doing for Congressional Affairs.

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975

b2
b6
b7C

[redacted]

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Wednesday, March 16, 2005 3:39 PM
To: [redacted]OCA) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

If you need operational examples please get them through [redacted]and [redacted]

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975

[redacted] b2 b6 b7C
Unclassified Fax: [redacted]
Secure Fax: [redacted]

-----Original Message-----
From: [redacted] OCA) (FBI)
Sent: Wednesday, March 16, 2005 3:36 PM
To: [redacted] (OGC) (FBI)
Cc [redacted] OGC) (FBI); Caproni, Valerie E. (OGC) (FBI); [redacted] (OCA) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: Draft Testimony re Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] attached is some info that might assist in drafting testimony.

b5 [redacted]

After you've had a chance to review, please give me a call and we can chat.

[redacted]
Special Counsel
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] RMD) (FBI)

From: [redacted] (OGC)(FBI)
Sent: Wednesday, March 23, 2005 11:39 AM
To: [redacted] (OGC) (FBI)
Subject: FW: ITOS I PATRIOT ACT RESPONSES

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted] (CTD)(FBI)
Sent: Tuesday, March 22, 2005 5:32 PM
To: [redacted] OGC)(FBI); [redacted] (CTD) (FBI)
Cc: [redacted] (CTD) (FBI)
Subject: ITOS I PATRIOT ACT RESPONSES

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Attached is the combined response from ITOS I of Patriot Act Successes.

Thanks,

[redacted]
CTD/ITOS 1/CONUS 1
[redacted]

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179dmh/baw 05-cv-0845

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted](RMD) (FBI)

From: [redacted](OGC)(FBI)
Sent: Tuesday, March 22, 2005 5:07 PM
To: [redacted](OGC) (FBI)
Subject: FW: Patriot Act issues for Conus 2

b6
b7C

SECRET//ORCON,NOFORN
RECORD adm

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-12-2005 BY 65179dmh/baw 05-cv-0845

-----Original Message-----
From: [redacted](CTD) (FBI)
Sent: Tuesday, March 22, 2005 2:14 PM
To: [redacted]OGC)(FBI)
Cc: [redacted](CTD) (FBI); [redacted](CTD) (FBI)
Subject: Patriot Act issues for Conus 2

b6
b7C

SECRET//ORCON,NOFORN
RECORD adm

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20150322
SECRET//ORCON,NOFORN

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20150322
SECRET//ORCON,NOFORN

[redacted] RMD) (FBI)

From: [redacted] (CTD) (FBI)
Sent: Tuesday, March 22, 2005 5:02 AM
To: [redacted] OGC)(FBI)
Cc: [redacted] CTD) (FBI)
Subject: FW: Request from EAD Bald

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

UNCLASSIFIED
NON-RECORD

DATE: 12-12-2005
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-12-2030

[redacted]

Can you look at the below e-mail? If you have already pulled some of this together, would you mind sending what you have to myself and SSA [redacted] EAD Bald has asked us to get this him, so he can forward to the Director.

Thank You,

[redacted]
CTD-Executive Staff

b6
b7C

-----Original Message-----
From: [redacted] CTD) (FBI)
Sent: Monday, March 21, 2005 6:58 PM
To: [redacted] (CTD) (FBI)
Cc: [redacted] OGC)(FBI) [redacted] (CTD) (FBI)
Subject: RE: Request from EAD Bald

UNCLASSIFIED
NON-RECORD

FYI [redacted] (OGC) requested the same info last week. I suggest you hook up with him, as maybe he can send you something already complete.

[redacted]

-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Monday, March 21, 2005 6:52 PM
To: [redacted] (CTD) (FBI); [redacted] (CTD) (FBI); [redacted] CTD) (FBI); [redacted] (CTD) (FBI); [redacted] (CTD)(FBI); [redacted] (CTD) (FBI); [redacted] (CTD) (FBI) [redacted] (CTD) (FBI) [redacted] CTD) (FBI); [redacted] OGC) (FBI)
Cc: [redacted] (CTD) (FBI)
Subject: Request from EAD Bald
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

To All,

Director Mueller has asked EAD Bald to give him examples of where the PATRIOT Act was used, and

b1
b6 its ability to make a difference in a case. One example mentioned was the [redacted] The
b7C Director would like to highlight the provision of the Act that these examples pertain too. EAD Bald wants
b2 this by noon on 3/24/05, so CTD Executive Staff requests the answers by **COB on 3/23/2005**. (S)

Please send your sections responses, positive or negative, to **SSA** [redacted] who will be coordinating this for EAD Bald.

Thank you in advance, b6
b7C

[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

[redacted](RMD) (FBI)

From: [redacted]OGC)(FBI)
Sent: Tuesday, March 22, 2005 5:10 PM
To: [redacted](OGC) (FBI)
Subject: FW: Responses for Director's Testimony/Patriot Act

UNCLASSIFIED
RECORD 315N-SE

b6
b7C

-----Original Message-----
From: [redacted](CTD) (FBI)
Sent: Friday, March 18, 2005 7:20 PM
To: [redacted](CTD) (FBI)
Cc: [redacted](OGC)(FBI)
Subject: FW: Responses for Director's Testimony/Patriot Act

UNCLASSIFIED
RECORD 315N-SE

Patriot Act info

[redacted]

CTD/ITOS 1/Conus IV

[redacted]

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-12-2005 BY 65179DMH/BAW 05-cv-0845

-----Original Message-----
From: [redacted]CTD) (FBI)
Sent: Friday, March 18, 2005 11:15 AM
To: [redacted](CTD) (FBI)
Cc: [redacted](CTD) (FBI)
Subject: Responses for Director's Testimony/Patriot Act

UNCLASSIFIED
RECORD 315N-SE

[redacted]

[redacted]asked that we provide examples of Patriot Act info/examples from our division's of responsibility, which are being compiled for the director's testimony. This is a [redacted]example of timely criminal investigative/intel info sharing with the Department of Defense (Army):

(U[redacted]

b2
b6
b7C
b7E

[redacted]

b2
b7E
b6
b7C

[redacted]

Thanks for passing this along. [redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] **(RMD) (FBI)**

From: [redacted] (CTD)(FBI) b6 b7C
Sent: Tuesday, March 22, 2005 5:32 PM
To: [redacted] (OGC)(FBI); [redacted] (CTD) (FBI)
Cc: [redacted] (CTD) (FBI)
Subject: ITOS I PATRIOT ACT RESPONSES

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Attached is the combined response from ITOS I of Patriot Act Successes.

Thanks,

[redacted]
CTD/ITOS 1/CONUS 1 b2
[redacted] b6
b7C

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-12-2005 BY 65179DMH/baw 05-cv-0845

[redacted] (RMD) (FBI)

From: [redacted] (CTD) (FBI) b6
Sent: Tuesday, March 22, 2005 2:14 PM b7C
To: [redacted] OGC)(FBI)
Cc: [redacted] (CTD) (FBI) [redacted] CTD) (FBI)
Subject: Patriot Act issues for Conus 2

SECRET//ORCON,NOFORN
RECORD adm

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFY ON: 20150322
SECRET//ORCON,NOFORN

DECLASSIFIED BY 65179dmh/baw 05-cv-0845
ON 12-12-2005

[redacted] (RMD) (FBI)

From: [redacted] (CTD) (FBI)
Sent: Monday, March 21, 2005 12:53 PM
To: [redacted] CTD) (FBI)
Cc: [redacted] (OGC)(FBI)
Subject: RE: Bullets for Director's Senate Testimony

b6
b7C

DATE: 12-12-2005
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C,D)
DECLASSIFY ON: 12-12-2030

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Thanks [redacted] is handling that, I'm not doing anything about the Patriot Act tasking.

[redacted]
CTD/ITOS-1
[redacted]

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Friday, March 18, 2005 7:18 PM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (OGC)(FBI)
Subject: FW: Bullets for Director's Senate Testimony

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Patriot Act tasking

[redacted]
Unit Chief
CTD/ITOS 1/Conus IV
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] CTD) (FBI)
Sent: Friday, March 18, 2005 11:01 AM
To: [redacted] CTD) (FBI)
Cc: [redacted] CTD) (FBI); [redacted] (CTD) (FBI); [redacted] (CTD) (FBI)
Subject: Bullets for Director's Senate Testimony

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Here is a bullet for th[redacted]ivision:

b1
b2
b7E
b6
b7C

(U) [redacted]

(S)

Thanks,

[redacted]

IA [redacted]
CTD/ITOS I/CONUS IV

[redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SECRET

[redacted] (RMD) (FBI)

From: [redacted] OGC)(FBI)
Sent: Thursday, March 17, 2005 9:58 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-12-2005 BY 65179dmh/baw 05-cv-0845

[redacted]

I've received the attached, and I'll be glad to assist.

I plan to contact our ITOS I folks ASAP. In the meantime, if there are any documents or other e-mails that weren't included in the e-mails forwarded to me, please pass them along.

Thanks.

[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 17, 2005 9:26 AM
To [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); DILLINGHAM, WAYNE E (OGC)(FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted]

CTLU I will gladly assist. I will have [redacted] reach out to ITOS I and see what we can drum up for you. [redacted]

b6
b7C

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Thursday, March 17, 2005 7:30 AM
To [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] OGC) (FBI); [redacted] OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

Here is the e-mail which [redacted] is responding to

b6
b7C

Do we have PAtriot Act successes.

-----Original Message-----
From [redacted] (OCA) (FBI)
Sent: Wednesday, March 16, 2005 2:49 PM
To: [redacted] OGC) (FBI)
b6 **Cc:** [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); Caproni, Valerie E. (OGC) (FBI)
b7C **Subject:** RE: Two things

UNCLASSIFIED
NON-RECORD

[redacted] it sounds like you've got the ticket to start drafting testimony for the Director to use for the Senate Judiciary Committee Patriot Act hearing scheduled for 4/5/2005. See attached e-mail to GC Caproni with relevant dates - OCA needs to see a draft of the testimony by Tues, 3/22.

b5 [redacted]

Give me a call to discuss. Thanks,

[redacted]
National Security Law Policy and Training Unit
FBI HQ Room 7975
[redacted]
Unclassified Fax [redacted]
Secure Fax: [redacted]

-----Original Message-----
b2 **From** [redacted] (OGC) (FBI)
b6 **Sent:** Thursday, March 17, 2005 7:26 AM
b7C **To:** [redacted] OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI) [redacted] OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

Could you get operaitonal examples for [redacted] for this project which we are doing for Congressional Affairs.

[redacted]
National Security Law Policy and Training Unit

FBI HQ Room 7975

b2
b6
b7C

-----Original Message-----
From (OGC) (FBI)
Sent: Wednesday, March 16, 2005 3:39 PM
To: (OCA) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

If you need operational examples please get them throug

National Security Law Policy and Training Unit
FBI HQ Room 7975

b2 Unclassified Fax:
b6 Secure Fax:
b7C

-----Original Message-----
From OCA) (FBI)
Sent: Wednesday, March 16, 2005 3:36 PM
To (OGC) (FBI)
Cc (OGC) (FBI); Caproni, Valerie E. (OGC) (FBI)
OCA) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

b6 b7C attached is some info that might assist in drafting testimony.

b5

After you've had a chance to review, please give me a call and we can chat.

b6
b7C

Special Counsel
Office of Congressional Affairs

[redacted] b2

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (RMD) (FBI)

From: [redacted] OGC) (FBI) b6 b7C

Sent: Thursday, March 17, 2005 9:26 AM

To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI) [redacted]
[redacted] (OGC) (FBI) [redacted] (OGC)(FBI)

Subject: RE: Draft Testimony re Patriot Act

Follow Up Flag: Follow up

Flag Status: Flagged

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-12-2005 BY 65179dmh/baw 05-cv-0845

UNCLASSIFIED
NON-RECORD

[redacted]

CTLLL I will gladly assist. I will have [redacted] reach out to ITOS I and see what we can drum up for you.

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 17, 2005 7:30 AM
b6 **To:** [redacted] OGC) (FBI); [redacted] (OGC) (FBI); [redacted] OGC) (FBI);
b7C [redacted] OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

Here is the e-mail which [redacted] is responding to

Do we have PAtriot Act successes.

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Wednesday, March 16, 2005 2:49 PM
To: [redacted] (OGC) (FBI)
b6 **Cc:** [redacted] GC) (FBI); THOMAS, JULIE F. (OGC) (FBI); Caproni, Valerie E. (OGC) (FBI)
b7C **Subject:** RE: Two things

UNCLASSIFIED
NON-RECORD

[redacted] it sounds like you've got the ticket to start drafting testimony for the Director to use for the Senate Judiciary Committee Patriot Act hearing scheduled for 4/5/2005. See attached e-mail to GC Caproni with relevant dates - OCA needs to see a draft of the testimony by Tues, 3/22.

b5 [redacted]

Give me a call to discuss. Thanks,

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975
[redacted]
Unclassified Fax: [redacted]
b2 Secure Fax: [redacted]
b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 17, 2005 7:26 AM
To: [redacted] OGC) (FBI); [redacted] OGC) (FBI) [redacted] OGC) (FBI) [redacted] OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

Could you get operaitonal examples for [redacted] for this project which we are doing for Congressional Affairs.

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975
[redacted]
Unclassified Fax: [redacted]
Secure Fax: [redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Wednesday, March 16, 2005 3:39 PM
To: [redacted] CA) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted]

b2 If you need operational examples please get them through [redacted]
b6
b7C [redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975
[redacted]
Unclassified Fax [redacted]

Secure Fa[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted]OCA) (FBI)
Sent: Wednesday, March 16, 2005 3:36 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted]GC) (FBI); Caproni, Valerie E. (OGC) (FBI); [redacted]
P. (OCA) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

b6 b7C [redacted] attached is some info that might assist in drafting testimony.

b5 [redacted]

After you've had a chance to review, please give me a call and we can chat.

b2 [redacted]
b6 Special Counsel
b7C Office of Congressional Affairs
[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 14
Page 2 ~ Duplicate
Page 3 ~ Duplicate
Page 11 ~ Duplicate
Page 12 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 19 ~ Duplicate
Page 20 ~ Duplicate
Page 21 ~ Duplicate
Page 27 ~ Duplicate
Page 33 ~ Duplicate
Page 34 ~ Duplicate
Page 35 ~ Duplicate
Page 37 ~ Duplicate

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 67
Page 6 ~ b1, b2, b6, b7C, b7D, b7E
Page 7 ~ b1, b2, b6, b7C, b7D, b7E
Page 8 ~ b1, b2, b6, b7A, b7C, b7E
Page 9 ~ b1, b2, b6, b7C, b7E
Page 10 ~ b1, b2, b6, b7C, b7E
Page 11 ~ b1, b2, b6, b7C, b7E
Page 12 ~ b1, b2, b6, b7C, b7E
Page 13 ~ b1, b2, b6, b7C, b7E
Page 14 ~ b1, b2, b6, b7C, b7E
Page 15 ~ b1, b2, b6, b7C, b7E
Page 16 ~ b1, b2, b6, b7C, b7E
Page 17 ~ b1, b2, b6, b7C, b7E
Page 18 ~ b1, b2, b6, b7C, b7E
Page 19 ~ b1, b2, b6, b7C, b7E
Page 20 ~ b1, b2, b6, b7C, b7E
Page 21 ~ b1, b2, b6, b7C, b7E
Page 22 ~ b1, b2, b6, b7C, b7E
Page 23 ~ b1, b2, b6, b7C, b7E
Page 24 ~ b1, b2, b6, b7C, b7E
Page 25 ~ b1, b2, b6, b7C, b7E
Page 26 ~ b1, b2, b7E
Page 27 ~ b1, b2, b6, b7C, b7D, b7E
Page 28 ~ b1, b2, b6, b7C, b7D, b7E
Page 29 ~ b1, b2, b6, b7C, b7D, b7E
Page 30 ~ b1, b2, b6, b7C, b7D, b7E
Page 31 ~ b1, b2, b6, b7C, b7E
Page 32 ~ Duplicate
Page 33 ~ b1, b2, b6, b7C, b7E
Page 34 ~ b1, b2, b6, b7C, b7E
Page 35 ~ b1, b2, b6, b7C, b7E
Page 36 ~ Duplicate
Page 37 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 38 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 39 ~ b1, b2, b6, b7C, b7E
Page 40 ~ b1, b2, b6, b7C, b7E
Page 41 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 42 ~ b1, b2, b6, b7A, b7C, b7D
Page 43 ~ b1, b2, b6, b7C, b7E
Page 44 ~ Duplicate
Page 45 ~ b1, b2, b6, b7C, b7E
Page 46 ~ b1, b2, b6, b7C, b7E
Page 47 ~ b1, b2, b6, b7C, b7E
Page 48 ~ b1, b2, b6, b7C, b7E
Page 49 ~ b1, b2, b6, b7C, b7E

Page 50 ~ b1, b2, b6, b7C, b7E
Page 51 ~ b1, b2, b6, b7C, b7E
Page 52 ~ b1, b2, b6, b7A, b7C, b7E
Page 53 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 54 ~ b1, b2, b6, b7C, b7D, b7E
Page 55 ~ b1, b2, b6, b7C, b7E
Page 56 ~ b1, b2, b6, b7C, b7E
Page 57 ~ b1, b2, b6, b7C, b7E
Page 58 ~ b1, b2, b6, b7C, b7D, b7E
Page 59 ~ Duplicate
Page 60 ~ b1, b2, b6, b7C, b7E
Page 61 ~ b1, b2, b6, b7C, b7D, b7E
Page 62 ~ b1, b2, b6, b7C, b7E
Page 63 ~ b1, b2, b6, b7C, b7E
Page 64 ~ b1, b2, b6, b7C, b7E
Page 65 ~ b1, b2, b6, b7C, b7E
Page 66 ~ b1, b2, b6, b7A, b7C, b7E
Page 67 ~ b1, b2, b6, b7C, b7E
Page 68 ~ b1, b2, b6, b7C, b7E
Page 69 ~ b1, b2, b6, b7C, b7D, b7E
Page 70 ~ b1, b2, b6, b7C, b7E
Page 71 ~ b1, b2, b6, b7C, b7D, b7E
Page 72 ~ b1, b2, b6, b7A, b7C, b7D, b7E

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 111
Page 3 ~ b1, b2, b6, b7C, b7E
Page 4 ~ b1, b2, b6, b7C, b7E
Page 5 ~ b1, b2, b6, b7A, b7C, b7E
Page 6 ~ b1, b2, b6, b7C, b7E
Page 7 ~ b1, b2, b6, b7A, b7C, b7E
Page 8 ~ b1, b2, b6, b7A, b7C, b7E
Page 9 ~ b1, b2, b6, b7C, b7E
Page 10 ~ b1, b2, b6, b7C, b7E
Page 11 ~ b1, b2, b6, b7C, b7E
Page 12 ~ b1, b2, b6, b7C, b7E
Page 13 ~ b1, b2, b6, b7C, b7E
Page 14 ~ b1, b2, b6, b7C, b7E
Page 15 ~ b1, b2, b6, b7A, b7C, b7E
Page 16 ~ b1, b2, b6, b7C, b7E
Page 17 ~ b1, b2, b6, b7A, b7C, b7E
Page 18 ~ b1, b2, b6, b7C, b7E
Page 19 ~ b1, b2, b6, b7C, b7E
Page 20 ~ b1, b2, b6, b7C, b7E
Page 21 ~ b1, b2, b6, b7C, b7E
Page 22 ~ b1, b2, b6, b7A, b7C, b7E
Page 23 ~ b1, b2, b6, b7C, b7E
Page 24 ~ b1, b2, b6, b7C, b7E
Page 25 ~ b1, b2, b6, b7C, b7E
Page 26 ~ b1, b2, b6, b7C, b7E
Page 27 ~ b1, b2, b6, b7C
Page 28 ~ b1, b2, b6, b7C, b7E
Page 29 ~ b1, b2, b6, b7C, b7E
Page 30 ~ b1, b2, b6, b7C, b7E
Page 31 ~ b1, b2, b6, b7C, b7E
Page 32 ~ b1, b2, b6, b7C, b7E
Page 33 ~ b1, b2, b6, b7C, b7E
Page 34 ~ b1, b2, b6, b7C, b7E
Page 35 ~ b1, b2, b6, b7C, b7E
Page 36 ~ b1, b2, b6, b7A, b7C, b7E
Page 37 ~ b1, b2, b6, b7A, b7C, b7E
Page 38 ~ b1, b2, b6, b7A, b7C, b7E
Page 39 ~ b1, b2, b6, b7C, b7E
Page 40 ~ b1, b2, b6, b7A, b7C, b7E
Page 41 ~ b1, b2, b6, b7C, b7E
Page 42 ~ b1, b2, b6, b7C
Page 43 ~ b1, b2, b6, b7C, b7E
Page 44 ~ b1, b2, b6, b7C, b7E
Page 45 ~ b1, b2, b6, b7A, b7C, b7E
Page 46 ~ b1, b2, b6, b7A, b7C, b7E

Page 47 ~ b1, b2, b6, b7A, b7C, b7E
Page 48 ~ b1, b2, b6, b7C, b7E
Page 49 ~ b1, b2, b6, b7C, b7E
Page 50 ~ b1, b2, b6, b7C, b7E
Page 51 ~ b1, b2, b6, b7C, b7E
Page 52 ~ b1, b2, b6, b7C, b7E
Page 53 ~ b1, b2, b6, b7C, b7E
Page 54 ~ b1, b2, b6, b7C, b7E
Page 55 ~ b1, b2, b6, b7C, b7E
Page 56 ~ b1, b2, b6, b7C, b7E
Page 57 ~ b1, b2, b6, b7C, b7E
Page 58 ~ b1, b2, b6, b7C, b7E
Page 59 ~ b1, b2, b6, b7A, b7C, b7E
Page 60 ~ b1, b2, b6, b7C, b7E
Page 61 ~ b1, b2, b6, b7C, b7E
Page 62 ~ b1, b2, b6, b7C, b7E
Page 63 ~ b1, b2, b6, b7C, b7E
Page 64 ~ b1, b2, b6, b7C, b7E
Page 65 ~ b1, b2, b6, b7C, b7E
Page 66 ~ b1, b2, b6, b7C, b7E
Page 67 ~ b1, b2, b6, b7C, b7E
Page 68 ~ b1, b2, b6, b7C, b7E
Page 69 ~ b1, b2, b6, b7C, b7E
Page 70 ~ b1, b2, b6, b7C, b7E
Page 71 ~ b1, b2, b6, b7C, b7E
Page 72 ~ b1, b2, b6, b7C, b7E
Page 73 ~ b1, b2, b6, b7C, b7E
Page 74 ~ b1, b2, b6, b7C, b7E
Page 75 ~ b1, b2, b6, b7C, b7E
Page 76 ~ b1, b2, b6, b7C, b7E
Page 77 ~ b1, b2, b6, b7C, b7E
Page 78 ~ b1, b2, b6, b7C, b7E
Page 79 ~ b1, b2, b6, b7C, b7E
Page 80 ~ b1, b2, b6, b7C, b7E
Page 81 ~ b1, b2, b6, b7C, b7E
Page 82 ~ b1, b2, b6, b7C, b7E
Page 83 ~ b1, b2, b6, b7C, b7E
Page 84 ~ b1, b2, b6, b7C, b7E
Page 85 ~ b1, b2, b6, b7C, b7E
Page 86 ~ b1, b2, b6, b7C, b7E
Page 87 ~ b1, b2, b6, b7C, b7E
Page 88 ~ b1, b2, b6, b7C, b7E
Page 89 ~ b1, b2, b6, b7C, b7E
Page 90 ~ b1, b2, b6, b7C, b7E
Page 91 ~ b1, b2, b6, b7C, b7E
Page 92 ~ b1, b2, b6, b7C, b7E
Page 93 ~ b1, b2, b6, b7C, b7E
Page 94 ~ b1, b2, b6, b7C, b7E
Page 95 ~ b1, b2, b6, b7C, b7E
Page 96 ~ b1, b2, b6, b7C, b7E
Page 97 ~ b1, b2, b6, b7C, b7E

Page 98 ~ b1, b2, b6, b7C, b7E
Page 99 ~ b1, b2, b6, b7C, b7E
Page 100 ~ b1, b2, b6, b7C, b7E
Page 101 ~ b1, b2, b6, b7C, b7E
Page 102 ~ b1, b2, b6, b7C, b7E
Page 103 ~ b1, b2, b6, b7C, b7E
Page 104 ~ b1, b2, b6, b7C, b7E
Page 105 ~ b1, b2, b6, b7C, b7E
Page 106 ~ b1, b2, b6, b7C, b7E
Page 107 ~ b1, b2, b6, b7C, b7E
Page 108 ~ b1, b2, b6, b7C, b7E
Page 109 ~ b1, b2, b6, b7C, b7E
Page 110 ~ b1, b2, b6, b7C, b7E
Page 111 ~ b1, b2, b6, b7C, b7E
Page 112 ~ b1, b2, b6, b7C, b7E
Page 113 ~ b1, b2, b6, b7C, b7E

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 85
Page 5 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 6 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 7 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 8 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 9 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 10 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 11 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 12 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 13 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 14 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 15 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 16 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 17 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 18 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 19 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 20 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 21 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 22 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 23 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 24 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 25 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 26 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 27 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 28 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 29 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 30 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 31 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 32 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 33 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 34 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 35 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 36 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 37 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 38 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 39 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 40 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 41 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 42 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 43 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 44 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 45 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 46 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 47 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 48 ~ b1, b2, b6, b7A, b7C, b7D, b7E

Page 49 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 50 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 51 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 52 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 53 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 54 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 55 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 56 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 57 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 58 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 59 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 60 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 61 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 62 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 63 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 64 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 65 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 66 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 67 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 68 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 69 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 70 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 71 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 72 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 73 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 74 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 75 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 76 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 77 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 78 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 79 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 80 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 81 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 82 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 83 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 84 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 85 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 86 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 87 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 88 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 89 ~ b1, b2, b6, b7A, b7C, b7D, b7E

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

[redacted]

b1

b2

b7E

DATE: 12-09-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-09-2030

James Baker
Counsel
Department of Justice
Office of Intelligence Policy and Review
950 Constitution Avenue, NW
Washington D.C. 20530

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

RE: Request for electronic surveillance and search authority of [redacted] pursuant to the Foreign Intelligence Surveillance Act (FISA). (S)

Dear Mr. Baker:

[redacted]

b1
b2
b7E

~~Derived From: G-3~~
~~Declassify On: X1~~

b1
b6
b7C
b2
b7E

SECRET

b1

b2

b7E

SECRET

SECRET

SECRET

[redacted] (S)

b1

Sincerely,

b2

b7E

[redacted]

b2

b7E

SECRET

~~SECRET~~

DEFINITION 1

This surveillance will INSERT - also be effected by the following means that, depending upon the technical requirements of the particular system involved, [redacted] b2 b7E [redacted] as described below:

[redacted] b1 b2 b7E

[AS OF JUNE 3, 2003: THIS DEFINITION SHOULD BE USED FOR THE FOLLOWING PROVIDERS [redacted] b2 b7E

~~SECRET~~

DEFINITION 2

This electronic surveillance will be effected by the following means, which [redacted] b2 b7E

[redacted] (S)

[redacted] b1 b2 b7E

[redacted]

b1
b2
b7E

[AS OF JUNE 3, 2003: THIS DEFINITION SHOULD BE USED FOR THE FOLLOWING PROVIDER(S) - [redacted]

b2
b7E

DEFINITION 3

This electronic surveillance will be effected by the following means, which [redacted] b2 b7E

[redacted] (S)

[redacted] b1 b2 b7E

[redacted] b1 b2 b7E

[redacted] (S) [Note to Drafter: Exhibit A must describe the reasons FBI needs to use an FBI-controlled device in each particular case, such as the [redacted] b2 b7E

[redacted]

[AS OF JUNE 3, 2003: THIS DEFINITION SHOULD BE USED FOR THE FOLLOWING PROVIDER(S) - [redacted] b2 b7E

[redacted]

Order a fe
Parts to be
respons
(8 Motion
top 8

Sharing Investigative Information with the Intelligence Community

A New Day In the IC-LE Relationship

[redacted]
Central Intelligence Agency

SSA [redacted]
Investigative Law Unit
Federal Bureau of Investigation
[redacted]

[redacted]
Counsel
OAAG, Criminal Division
U.S. Department of Justice
[redacted]

b2
b6
b7C

REFERENCE MATERIALS

- USA PATRIOT Act (extract)
- Homeland Security Act (extract)
- 18 U.S.C. § 2517 (as amended)
- Rule 6 (e), Fed. R. Crim. P. (as amended)
- Attorney General Guidelines
- PowerPoint Presentation

HOW THE USA PATRIOT ACT HAS HELPED THE FBI

I. Investigative Tools

Obtaining Voice Mail and Other Stored Voice Communications

Voice Mail - Under Section 209, law enforcement can now obtain all voice mail which is stored by a communications provider, [redacted] using the procedures set forth in 18 U.S.C. §2703 (such as a search warrant). [redacted] This tool will expire under the sunset provision. It should be noted that voice messages stored and in the possession of the user, such as communications stored on an answering machine, are not covered by the amended statute. See 18 U.S.C. § 2510; 18 U.S.C. § 2703.

b2
b7E
b5

Basic Subscriber Information - Under Section 210, the list of information which law enforcement can obtain with a subpoena was expanded to include records of session times and durations, any temporarily assigned network address, and the means and source of payment that a customer uses to pay for his/her account with a communications provider. 18 U.S.C. § 2703(c).

Nationwide Search Warrants for E-mail - Section 220 enables courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider. [redacted] Previously, the search warrant had to be issued by a court in the district where the service provider was located. This tool will also expire under the sunset provision. 18 U.S.C. § 2703.

b2
b7E

Clarification of the Cable Act - In the past there were two statutory standards for privacy protection: one governing cable service (47 U.S.C. § 551, the "Cable Service Act"), and the other governing telephone and Internet privacy (18 U.S.C. § 2510, *et seq.* [wiretap statute], 18 U.S.C. § 2701, *et seq.* [ECPA], 18 U.S.C. § 3121 *et seq.* [pen/trap statute]). This opened the door for cable companies which provide telephone and Internet services to argue that the ECPA, wiretap, and pen/trap statutes did not apply to them. Section 211 of the Patriot Act clarified this issue by stating that the ECPA, wiretap, and pen/trap statutes govern disclosures by cable companies that relate to the provision of communication services. See 47 U.S.C. § 551(c)(2)(D).

Voluntary Disclosures - Section 212 of the Patriot Act now explicitly permits (but does not require) a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers. The Act also allows a communications service provider to disclose non-content records to protect their rights and property. This will most often be used when the communications service provider itself is a victim of computer hacking. This provision will expire under the sunset provision. See 18 U.S.C. § 2702(b) & (c)(3); 18 U.S.C. § 2703(c)(2)(F).

Electronic Surveillance

Expanded Predicates for Title III - The predicate offenses for Title III were expanded to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). These also are set to expire under the sunset provision. See 18 U.S.C. § 2516.

Nationwide Effect of Pen/Trap Orders - The Act amends the pen/trap statute to give federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order. See 18 U.S.C. § 3127(2). Moreover, the amendments to the law clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information -- i.e. [redacted] -- used in the processing and transmitting of wire and electronic communications [redacted] b2 b7E

For example, a federal prosecutor may now obtain an order to trace calls made to a telephone within the prosecutor's local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, however, investigators still have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path to convey to the next carrier in the chain. The investigator then serves the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier then provides the connection information in its possession for the communication. The investigator must repeat this process until the order had been served on the originating carrier who was able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

Intercepting Communications of Computer Trespassers - The wiretap statute was amended by Section 217 to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the communications sent or received by trespassers. Thus, this section would only apply where the

configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer. Additionally, based on the definition of a "computer trespasser," communications of users who have a contractual relationship with the computer owner may not be monitored, even if their use is in violation of their contract terms (i.e. spammers). This is set to expire under the sunset provision. See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

Pen Register/Trap and Trace Reporting Requirement - Section 216 of the Act created a new reporting requirement whenever the government uses its own pen register or trap and trace equipment on a packet-switched data network of an electronic communications service to the public. While this provision was aimed at the use of the DCS-1000 (earlier versions were known as "Carnivore"), it will also apply to the use of other government owned equipment/software on a service provider's network. This new requirement imposes a duty to maintain records relating to the use of this equipment and to file these records with the court which authorized the pen register or trap and trace. See 18 U.S.C. § 3123(a)(3).

Search Warrants

Delayed Notice for Search Warrants - The Act created a uniform statutory standard authorizing courts to delay the provision of required notice if the court finds "reasonable cause" to believe that providing immediate notification of the execution of the warrant may have an adverse result as defined by 18 U.S.C. § 2705 (including endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation or unduly delaying a trial). The Act provides for the giving of notice within a "reasonable period" of a warrant's execution, which period can be further extended by a court for good cause. See 18 U.S.C. § 3103a.

Single Jurisdiction Search Warrants for Terrorism - Under prior law, Rule 41(a) of the Federal Rules of Criminal Procedure required that a search warrant be obtained with a district for searches conducted with that district. The only exception was for cases in which property or a person within the district might leave the district prior to the execution of the warrant. The rule created unnecessary delays and burdens for the government in the investigation of terrorism activities and networks that spanned a number of districts.

Section 219 resolves this problem by providing that, in domestic and international terrorism cases, a search warrant may be issued by a magistrate judge in any district in which activities related to terrorism have occurred for a search of property or persons located within or outside of the district.

Miscellaneous Tools

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 04/15/2003

To: All Field Offices **Attn:** ADIC
SAC
CDC

From: Office of the General Counsel
Investigative Law Unit/Room
Contact:

Approved By: Kelley Patrick W PWK

Drafted By:

b2
b6
b7C

Case ID #: 66F-HQ-1085160 (Pending) -60
66F-HQ-1085159 (Pending) 52
66F-HQ-C1382989 (Pending) 8
66F-HQ-C1384970 -501

Title: Emergency Disclosures under ECPA
18 U.S.C. § 2702
Reporting Requirement

Synopsis: This EC advises receiving field offices of the reporting requirement under 18 U.S.C. Section 2702(b)(7) regarding any voluntary disclosures made by a service provider to the FBI under this emergency disclosure provision. Field offices must immediately report if they received any voluntary disclosures of content or records from service providers under this provision between January 24, 2003 and March 31, 2003. Negative reports are not required. Additional reports will be required at later dates.

Enclosure(s): Sample report

Details: The Electronic Communications Privacy Act (ECPA), codified in 18 U.S.C. § 2701, *et. seq.*, provides privacy protection for electronic communications, such as e-mail, and associated records. It also outlines the compulsory process that law enforcement can use to obtain both the content of communications and records held by an electronic communications service provider or a remote computing service. The USA Patriot Act created a voluntary disclosure provision which explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. 18 U.S.C. § 2702(b)(7); 18 U.S.C. § 2702(c)(4). The Homeland Security Act modified this provision and created a reporting requirement for every disclosure made under this provision.

b2
b7E

This EC provides guidance on the reporting requirement and notifies the field of urgent deadlines in order to ensure full compliance with the statutory deadlines. Further guidance will be issued in the near future on the use of the provision.

I. DISCLOSURE TO TTIC OF CRIMINAL INFORMATION OBTAINED IN INTERNATIONAL TERRORISM (315) CASES

A. Authorities and restrictions imposed by process

1. Federal Grand Jury (FGJ) Material may be disclosed to the Terrorist Threat Information Center (TTIC), as a component of the Intelligence Community (IC), pursuant to Section 203 (a) of the USA Patriot Act, which amended Rule 6(e), Federal Rules of Criminal Procedure; and, if it is "foreign intelligence," it must be disclosed to the Director of Central Intelligence (DCI), pursuant to Section 905 of the Patriot Act., which amended 50 U.S.C. § 102B. (U)

[redacted] (U)

b5

[redacted] (U)

[redacted]

[redacted]

[redacted] (U)

[redacted] b5

[redacted] (U)

2. Title III Material may be disclosed to TTIC, as a component of the IC, pursuant to Section 203 (b) of the Patriot Act, which amended 18 U.S.C. § 2517 (6), which permits, but does not require, the disclosure of foreign intelligence, counter-intelligence, or foreign intelligence information (as defined in 18 U.S.C. § 2510) to federal intelligence officials. In addition, 50 U.S.C. § 102B requires disclosure of foreign intelligence to the DCI acquired during a criminal investigation (which would include foreign intelligence information acquired by a Title III intercept). (U)

[redacted] b5

[redacted] (U)

[redacted]

[redacted] (U) b5

[redacted] (U)

3. Other Criminal Processes: The following processes--by which evidence or other information is obtained in the course of a criminal investigation--impose no statutory or regulatory restrictions or marking or notice requirements that would affect disclosure of the information to TTIC and the IC. Although there is no process-specific statutory authority to share this information, the general authority to share with the IC foreign intelligence, counter-intelligence, or foreign intelligence information obtained in a criminal investigation pursuant to Section 203 (d) of the USA Patriot Act and the requirement to share foreign intelligence with the DCI pursuant 50 U.S.C. § 102B would certainly apply to disclosure to TTIC of such information produced by these processes that falls within these categories. (U)

a. Pen Register and Trap and Trace Information obtained under the authority of 18 U.S.C. §§ 3121 through 3127. (Disclosure of FISA Pen Register and Trace and Trace Information is governed by 50 U.S.C. § 1845.) (U)

b. Stored Electronic Communications obtained under the authority of 18 U.S.C. §§ 2701-2704. (U)

c. Administrative Subpoenas issued under the authority of 21 U.S.C. § 876 (for drug investigations) and 18 U.S.C. § 3486 (for health care fraud and child sexual exploitation investigations). (U)

d. Search Warrants pursuant to Rule 41, Federal Rules of Criminal Procedure. (U)

[redacted] b5

(FISA)

[redacted] b1

[redacted] (S) b1

[redacted] b1

[redacted] (S)

Markings: Pursuant to 50 U.S.C. § 1806(b), FISA information cannot be disclosed to TTIC for law enforcement purposes unless the disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General. (U)

[redacted] b1

[redacted] (S)

[redacted] b1

[redacted] (S)

[redacted] (S)

b1
b5

C. **FISA pen register and trap and trace devices, 50 U.S.C. § 1842, *et seq.***

Information concerning a United States person may be used and disclosed by Federal officers only in accordance with Section 1845. This section specifies that information acquired from a FISA pen register/trap and trace device may be disclosed to TTIC for lawful purposes. Any disclosure for law enforcement purposes must be accompanied by a statement that such information, or information derived therefrom, may not be used in a criminal proceeding without the advance authorization of the Attorney General. There are no process requirements or other limitations on dissemination. (U)

D. **National Security Letters**

1. The NSIG provide that information obtained from National Security Letters issued under 15 U.S.C. § § 1681u, 12 U.S.C. § 3414, and 18 U.S.C. § 2709 may be disseminated in accordance with the general standards of the NSIG as set forth above in Section II.A.1., subject to any limitations within each statute itself. There are no marking or process requirements. (U)

a. Financial Records obtained pursuant to 12 U.S.C. § 3414 may be disclosed to TTIC only as provided in the NSIG and only if such information is clearly relevant to the authorized responsibilities of the receiving agency. (U)

b. Consumer information obtained pursuant to 15 U.S.C. § 1681u may be disseminated to TTIC only if such dissemination is necessary for the approval or conduct of a foreign counterintelligence investigation. (U)

c. Toll and transactional records obtained pursuant to 18 U.S.C. § 2709 may be disclosed to TTIC only as provided in the NSIG and only if such information is clearly relevant to the authorized responsibilities of the receiving agency. (U)

[redacted] (S)

b1 b6

b2 b7C

DATE: 12-10-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-10-2030

From: [redacted]
To: SPIKE (MARION) BOWMAN
Date: Sun, Mar 10, 2002 5:53 PM
Subject: [redacted] (S)

b6
b7C

Spike,

[redacted] (S)

b1
b2
b5

While all who reviewed the memo had similar thoughts, the attached is significantly (if not almost entirely) based upon the work product of [redacted] who took the time to actually put her thoughts/analysis on paper. (please make sure Larry knows of her contribution)

I'll be in tomorrow and expect this will be the topic du jour.

Sorry it took so long....things are busy down here.

[redacted]

b6
b7C

CC: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] (S)

b1
b2
b6
b7C

DATE: 12-10-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-10-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~/DRAFT

March 11, 2002

b6
b7C [redacted]

[redacted] (S)

b1
b2
b5

The Patriot Act, Section 212, amended 18 U.S.C. 2702 (b)(6)(C) to permit ISPs to disclose content or non-content based communications to law enforcement "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." The disclosure is voluntary, and the provider has no affirmative obligation to review customer communications to detect imminent dangers.

Section 212 also amended 18 U.S.C. 2702 (c)(3) to specifically allow for the disclosure

[redacted] (S)

b1
b2
b5

SECRET/DRAFT

of non-content customer records "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." Section (c) (4) was added to allow the disclosure of non-content records to a "governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." ISPs already had the authority to disclose content-based communications "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." 18 U.S.C. 2702 (b)(5).

The amendments in Section 212 will sunset on December 31, 2005. [redacted] b5

[redacted] (S)

[redacted] b1
b5

[redacted]

b1
(S) b2
b6
b7C

~~SECRET~~/DRAFT

b5

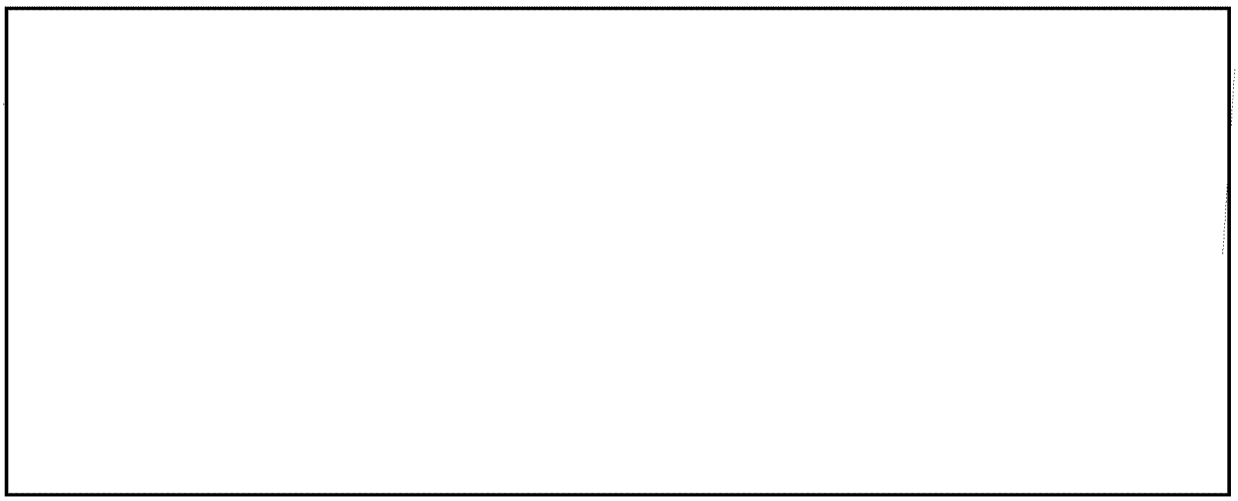
(S)

b1
b2
b5

b2
b5

b1
b2
(S)
b6
b7C

~~SECRET~~/DRAFT



(S)

b1
b2
b5

M.E. Bowman

Electronic Surveillance

Expanded Predicates for Title III - The predicate offenses for Title III were expanded to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). These also are set to expire under the sunset provision. See 18 U.S.C. § 2516.

Nationwide Effect of Pen/Trap Orders - The Act amends the pen/trap statute to give federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order. See 18 U.S.C. § 3127(2). Moreover, the amendments to the law clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information - [redacted] -- used in the processing and transmitting of wire and electronic communications [redacted] b2 b7E

For example, a federal prosecutor may now obtain an order to trace calls made to a telephone within the prosecutor's local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, however, investigators still have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path to convey to the next carrier in the chain. The investigator then serves the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier then provides the connection information in its possession for the communication. The investigator must repeat this process until the order had been served on the originating carrier who was able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

Intercepting Communications of Computer Trespassers - The wiretap statute was amended by Section 217 to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the

b6
b7C

From: SIOC ADMIN
To: All AO'S & OSM Employees Listing, All ASAC Employees Listing, ALL LEGAT GROUP, All SAC Employees Listing
Date: 3/18/02 9:07PM
Subject: Joint Intelligence Committee Inquiry

Understandably, there have been many questions generated by the EC that was sent out Friday night (3/15/02). Hopefully this e-mail will provide additional clarification.

When we asked for information responsive to the questions in referenced EC, it should only apply to information generated by or originated from your field office or Legat. If a field office received briefing material from HQ or another office which is OO, that information will be provided by HQ or that OO, respectively to the Congressional inquiry team.

Regarding Title III and 6(e) Material: There should not be much "Title III" for the classifications requested as the vast majority will be FISA. The USA Patriot Act, signed by President Bush on October 26, 2001, now allows the sharing of Title III and 6(e) Grand Jury material with the intelligence community, including those working intelligence investigations in the FBI. This law would permit the sharing of Title III and 6(e) material with HPSCI and SSCI. The Attorney General is drafting Guidelines on how to do this, however, they are not completed. In the interim, before Title III or 6(e) material is shared with anyone, including FBI employees, for intelligence purposes, the case agent in the field must go to his/her AUSA and explain why the information must be shared and with whom. The AUSA will then get an OK from the responsible Judge. Then, the information can be shared with those of us working the Task Force and with HPSCI and SSCI.

Regarding FISA material, that information should have been translated, reviewed for pertenence and the results transcibed unto "logs." Those logs should have been serialized in a subfile of the main investigative file or other pertinent file. If that material has not been uploaded into ACS, then it must be captured in this process.

As far as source information (134, 137, 270) : At this stage, we are not pulling and shipping asset/informant/CW files. We will work under the premise that pertinent and responsive information for this inquiry will be contained in a substantive investigative file which will be captured in that manner. If any office is aware of information that is responsive to the contrary, please advise.

On the list of classifications we provided, classification "283" did not exist until 10/1/93 so you won't have any cases under that file from 1/1/93 to 10/1/93. Disregard classification 163F.

Anything which has been uploaded into ACS or has been scanned or entered into INTELPLUS does not need to be sent to be scanned at this time. If you are unsure about information not being in either of those two formats, then it should be sent to the designated location for scanning.

Regarding the planned conference call with the Director, those details are still being worked out as he has been out of the country for the past week and a half. Details will be provided as soon as they are available.

Many of the phone calls we are receiving touch on a variety of topics ranging from (1) the specifics on the committee's inquiry, to (2) the technical aspects of the scanning project, to (3) ACS and document uploading in general. In an attempt to provide you with better point of contact (POC) information, you can either call or e-mail the following individuals with questions, respectively:

b2
b6
b7C

(1)
(2)
(3)

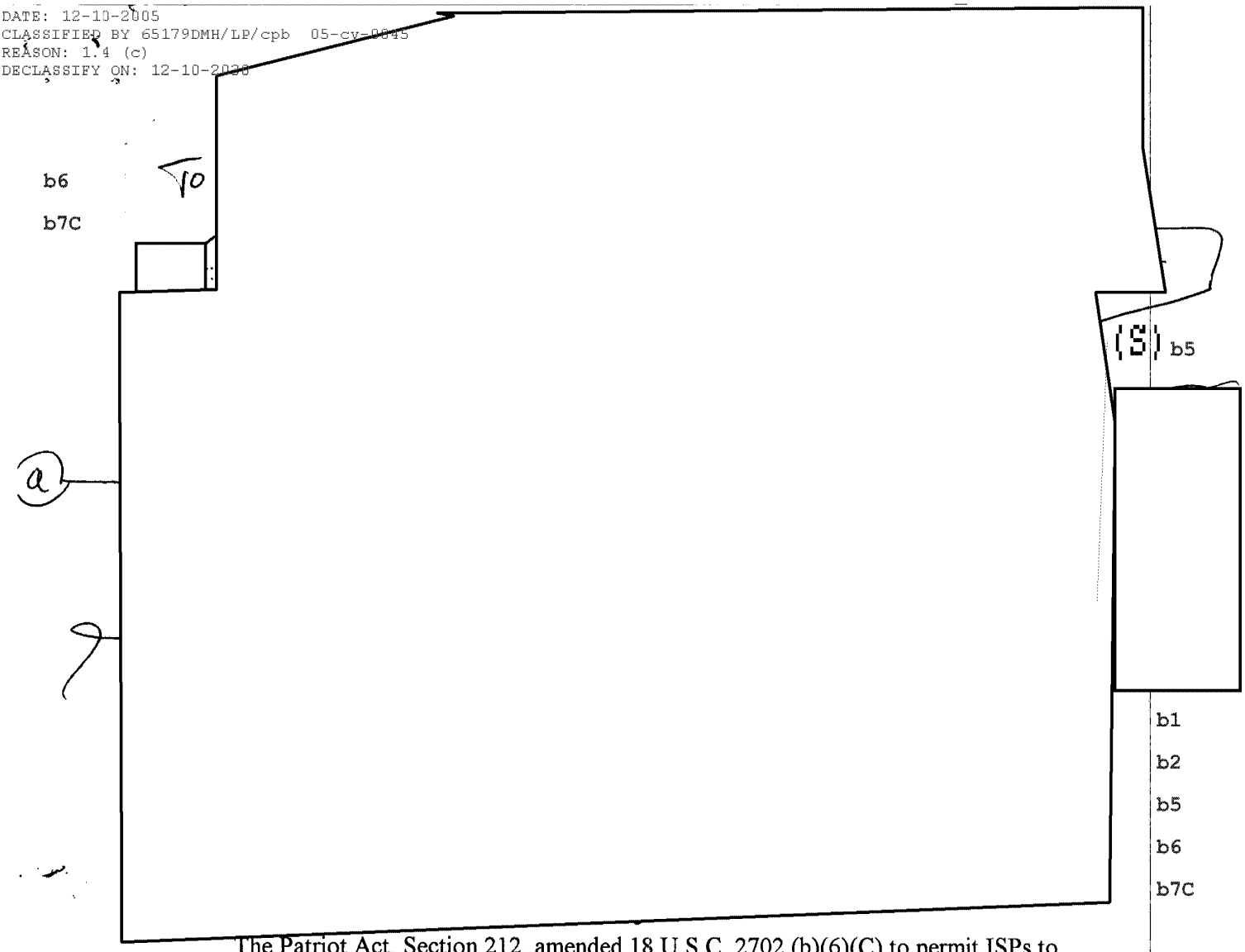
b6

b7C

[redacted] b2

Additional e-mails will be forthcoming to address questions and provide additional clarification. Thanks much for your efforts on this matter.

b6
b7C



b1
b2
b5
b6
b7C

The Patriot Act, Section 212, amended 18 U.S.C. 2702 (b)(6)(C) to permit ISPs to disclose content or non-content based communications to law enforcement "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." The disclosure is voluntary, and the provider has no affirmative obligation to review customer communications to detect imminent dangers.

b1
b2
b5

Section 212 also amended 18 U.S.C. 2702 (c)(3) to specifically allow for the disclosure

(S)

b5

of non-content customer records "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." Section (c) (4) was added to allow the disclosure of non-content records to a "governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." ISPs already had the authority to disclose content-based communications "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service." 18 U.S.C. 2702 (b)(5).

The amendments in Section 212 will sunset on December 31, 2005

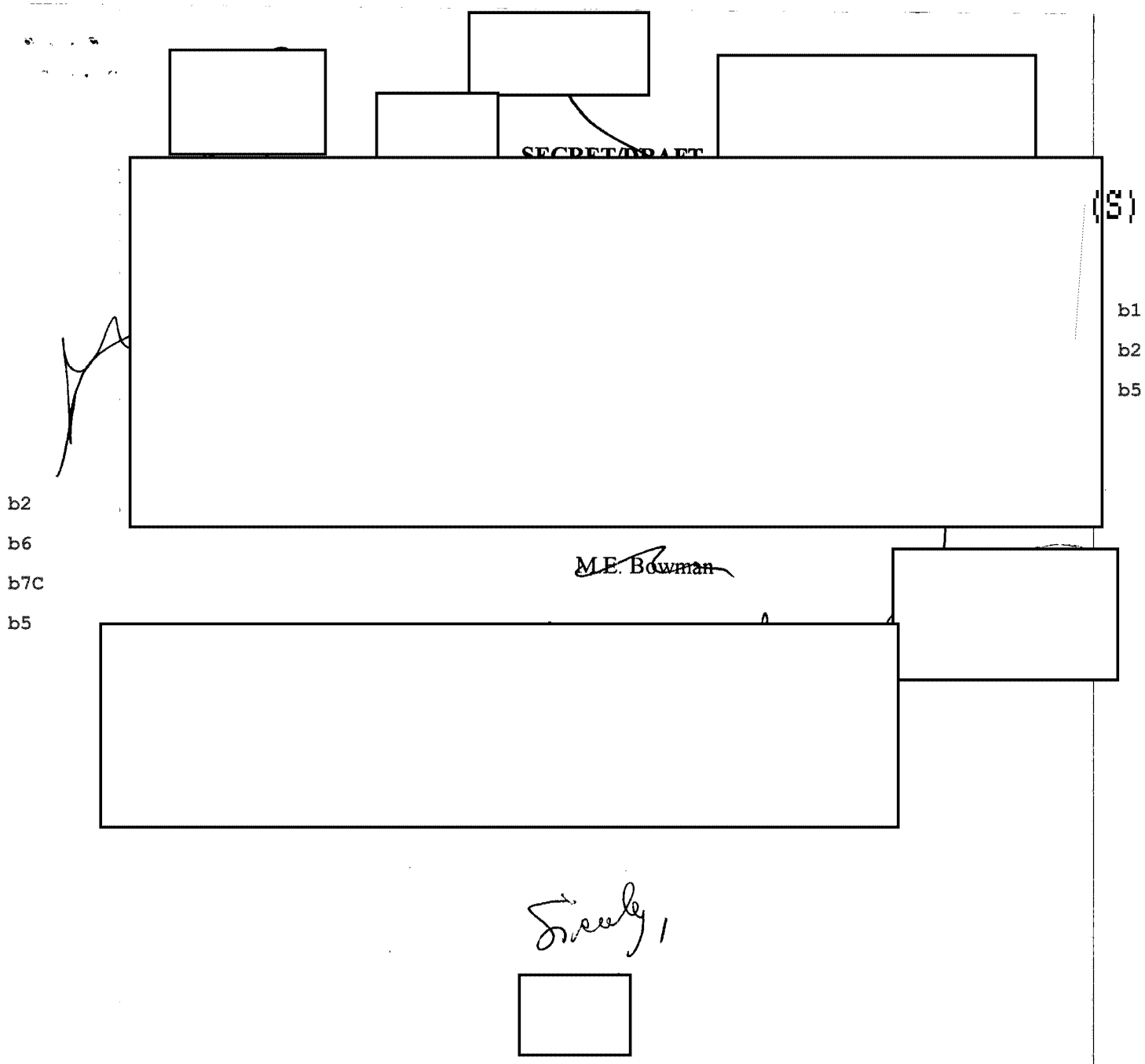
b5

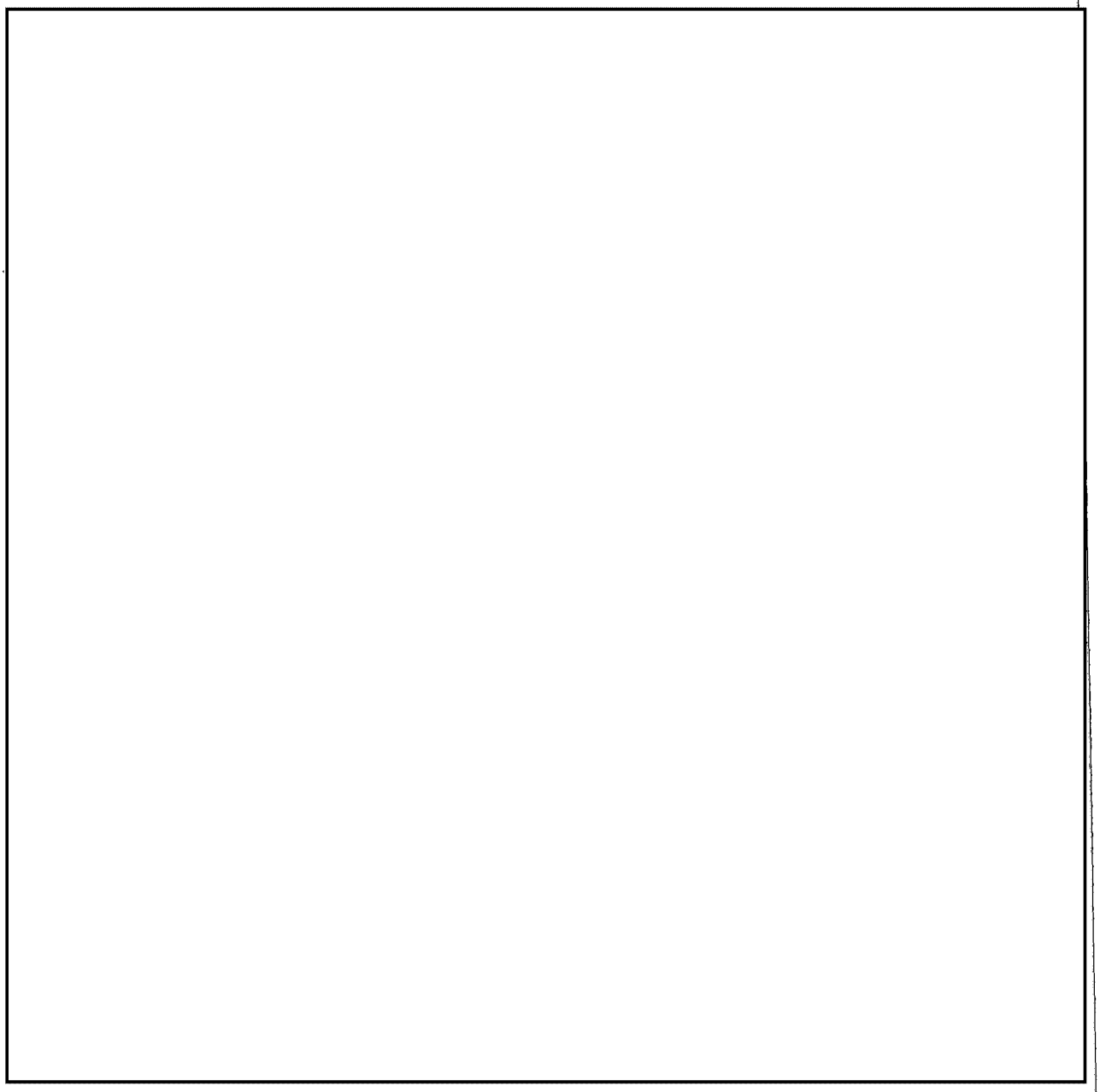
(S)

b1

b2

b5


SECRET//NOFORN
(S)
b1
b2
b5
b2
b6
b7C
b5
M.E. Bowman



b5

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 210
Page 1 ~ Referral/Direct
Page 2 ~ Referral/Direct
Page 12 ~ Duplicate
Page 13 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 16 ~ Duplicate
Page 17 ~ Duplicate
Page 18 ~ Duplicate
Page 19 ~ Duplicate
Page 20 ~ Duplicate
Page 21 ~ Duplicate
Page 22 ~ Duplicate
Page 23 ~ b2, b6, b7C, b7E
Page 24 ~ b2, b6, b7C, b7E
Page 25 ~ b2, b6, b7C, b7E
Page 26 ~ b2, b6, b7C, b7E
Page 27 ~ b2, b6, b7C, b7E
Page 28 ~ b2, b6, b7C, b7E
Page 29 ~ b2, b6, b7C, b7E
Page 30 ~ b2, b6, b7C, b7E
Page 46 ~ Referral/Direct
Page 47 ~ Referral/Direct
Page 48 ~ Referral/Direct
Page 49 ~ Referral/Direct
Page 50 ~ Referral/Direct
Page 51 ~ Referral/Direct
Page 52 ~ Referral/Direct
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 55 ~ Duplicate
Page 56 ~ Duplicate
Page 57 ~ Duplicate
Page 58 ~ Duplicate
Page 59 ~ Duplicate
Page 63 ~ Referral/Direct
Page 64 ~ Referral/Direct
Page 65 ~ Referral/Direct
Page 66 ~ Referral/Direct
Page 67 ~ Referral/Direct
Page 68 ~ Referral/Direct
Page 114 ~ Referral/Direct
Page 115 ~ Referral/Direct
Page 116 ~ Referral/Direct

Page 120 ~ Duplicate
Page 121 ~ Duplicate
Page 122 ~ Duplicate
Page 123 ~ Duplicate
Page 124 ~ Duplicate
Page 125 ~ Duplicate
Page 126 ~ Duplicate
Page 127 ~ Duplicate
Page 128 ~ Duplicate
Page 129 ~ Duplicate
Page 130 ~ Duplicate
Page 131 ~ Duplicate
Page 132 ~ Duplicate
Page 133 ~ Duplicate
Page 134 ~ Duplicate
Page 135 ~ Duplicate
Page 136 ~ Duplicate
Page 137 ~ Duplicate
Page 138 ~ Duplicate
Page 139 ~ Duplicate
Page 140 ~ Duplicate
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Duplicate
Page 145 ~ Duplicate
Page 146 ~ Duplicate
Page 147 ~ Duplicate
Page 148 ~ Duplicate
Page 149 ~ Duplicate
Page 150 ~ Duplicate
Page 151 ~ Duplicate
Page 152 ~ Duplicate
Page 153 ~ Duplicate
Page 154 ~ Duplicate
Page 155 ~ Duplicate
Page 156 ~ Duplicate
Page 157 ~ Duplicate
Page 158 ~ Duplicate
Page 159 ~ Duplicate
Page 160 ~ Duplicate
Page 161 ~ Duplicate
Page 162 ~ Duplicate
Page 163 ~ Duplicate
Page 164 ~ Duplicate
Page 165 ~ Duplicate
Page 166 ~ Duplicate
Page 167 ~ Duplicate
Page 168 ~ Duplicate
Page 169 ~ Duplicate
Page 170 ~ Duplicate

Page 171 ~ Duplicate
Page 172 ~ Duplicate
Page 173 ~ Duplicate
Page 174 ~ Duplicate
Page 175 ~ Duplicate
Page 176 ~ Duplicate
Page 177 ~ Duplicate
Page 178 ~ Duplicate
Page 179 ~ Duplicate
Page 180 ~ Duplicate
Page 181 ~ Duplicate
Page 220 ~ Duplicate
Page 221 ~ Duplicate
Page 222 ~ Duplicate
Page 223 ~ Duplicate
Page 224 ~ Duplicate
Page 225 ~ Duplicate
Page 226 ~ Duplicate
Page 227 ~ Duplicate
Page 228 ~ Duplicate
Page 229 ~ Duplicate
Page 230 ~ Duplicate
Page 248 ~ Referral/Direct
Page 249 ~ Referral/Direct
Page 250 ~ Referral/Direct
Page 251 ~ Referral/Direct
Page 252 ~ Referral/Direct
Page 253 ~ Referral/Direct
Page 254 ~ Referral/Direct
Page 255 ~ Referral/Direct
Page 256 ~ Referral/Direct
Page 257 ~ Referral/Direct
Page 258 ~ Referral/Direct
Page 259 ~ Referral/Direct
Page 260 ~ Referral/Direct
Page 261 ~ Referral/Direct
Page 262 ~ Referral/Direct
Page 263 ~ Referral/Direct
Page 264 ~ Referral/Direct
Page 265 ~ Referral/Direct
Page 266 ~ Referral/Direct
Page 267 ~ Referral/Direct
Page 268 ~ Referral/Direct
Page 270 ~ Duplicate
Page 271 ~ Duplicate
Page 272 ~ Duplicate
Page 273 ~ Duplicate
Page 277 ~ Duplicate
Page 278 ~ Duplicate
Page 279 ~ Duplicate
Page 280 ~ Duplicate

Page 281 ~ Duplicate
Page 282 ~ Duplicate
Page 283 ~ Duplicate
Page 284 ~ Duplicate
Page 285 ~ Duplicate
Page 286 ~ Duplicate
Page 299 ~ Duplicate
Page 300 ~ Duplicate
Page 301 ~ Duplicate
Page 302 ~ Duplicate
Page 303 ~ Duplicate
Page 306 ~ Referral/Direct
Page 307 ~ Referral/Direct
Page 308 ~ Referral/Direct
Page 309 ~ Referral/Direct
Page 310 ~ Referral/Direct
Page 311 ~ Referral/Direct
Page 312 ~ Referral/Direct
Page 313 ~ Referral/Direct
Page 314 ~ Referral/Direct
Page 315 ~ Referral/Direct
Page 316 ~ Referral/Direct
Page 317 ~ Referral/Direct
Page 318 ~ Referral/Direct
Page 319 ~ Referral/Direct
Page 320 ~ Referral/Direct
Page 321 ~ Referral/Direct
Page 322 ~ Referral/Direct
Page 323 ~ Referral/Direct
Page 324 ~ Referral/Direct
Page 325 ~ Referral/Direct
Page 326 ~ Referral/Direct
Page 327 ~ Referral/Direct
Page 328 ~ Referral/Direct
Page 329 ~ Referral/Direct
Page 341 ~ b1, b2, b5
Page 343 ~ Referral/Direct
Page 344 ~ Referral/Direct
Page 345 ~ Referral/Direct
Page 346 ~ Referral/Direct
Page 347 ~ Referral/Direct
Page 348 ~ Duplicate
Page 349 ~ Duplicate
Page 350 ~ Duplicate
Page 351 ~ Duplicate
Page 352 ~ Duplicate
Page 353 ~ Duplicate
Page 354 ~ Referral/Direct
Page 355 ~ Referral/Direct
Page 356 ~ Referral/Direct
Page 357 ~ Referral/Direct

Page 358 ~ Referral/Direct
Page 359 ~ Referral/Direct
Page 360 ~ Referral/Direct
Page 361 ~ Referral/Direct
Page 362 ~ Referral/Direct
Page 363 ~ Referral/Direct
Page 364 ~ Referral/Direct
Page 365 ~ Referral/Direct
Page 366 ~ Referral/Direct
Page 367 ~ Referral/Direct
Page 368 ~ Referral/Direct
Page 369 ~ Referral/Direct
Page 370 ~ Referral/Direct

[redacted](RMD) (FBI)

From: [redacted](OGC) (FBI) b2
Sent: Wednesday, February 23, 2005 11:41 AM b6
To: [redacted](OGC) (OGA) b7C
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report
Importance: High

UNCLASSIFIED
NON-RECORD

Did you work on this?

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975 b2
STU III: [redacted] b6
Unclassified Fax [redacted] b7C
Secure Fax [redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Wednesday, February 23, 2005 9:46 AM
To: [redacted](OGC) (FBI)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report
Importance: High

UNCLASSIFIED
NON-RECORD

[redacted]

I don't think so. But this is OBE anyway, because the deadline was yesterday.

[redacted] b6 b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Wednesday, February 23, 2005 8:36 AM
To: [redacted]OGC) (FBI)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

You commented right?

-----Original Message-----
From: [redacted] (OGC) (FBI) b6
Sent: Monday, February 21, 2005 2:51 PM b7C
To [redacted]OGC) (FBI)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

Did I already forward this to you? Haven't we already commented on this once? Julie
-----Original Message-----
From [redacted] (OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc [redacted] OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcmte on Terrorism and is meant to:
1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments t[redacted] ext[redacted] by **9:00 am, Tuesday, 2/22/05**.

Thanks for your assistance.

b2
b6
b7C

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (RMD) (FBI)

From: [redacted] (OGC) (OGA) b6
Sent: Wednesday, January 19, 2005 1:50 PM b7C
To: [redacted] (OGC) (FBI)
Subject: FW: sunset

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

FYI

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, January 19, 2005 1:49 PM
To: [redacted] (OGC) (OGA) b6
Cc: [redacted] (OCA) (FBI) b7C
Subject: RE: sunset

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179DMH/BAW 05-cv-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Great. [redacted] let me know if you need anything else from us. Julie b6 b7C

-----Original Message-----
From: [redacted] (OGC) (OGA)
Sent: Wednesday, January 19, 2005 1:46 PM
To: THOMAS, JULIE F. (OGC) (FBI) b6
Cc: [redacted] (OCA) (FBI) b7C
Subject: sunset

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Julie:

[redacted] and I just spoke and agreed that we would take out the sublist of USA Patriot Act provisions that will sunset and just refer to them generally. [redacted] will send DOJ our comments concerning the significant purpose standard in FISA.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (RMD) (FBI)

From: [redacted] (OGC) (OGA) b6 b7C
Sent: Wednesday, February 23, 2005 2:31 PM
To: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: sunset

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie [redacted]

This was done a few weeks ago -- see below.

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179DMH/BAW 05-cv-0845

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, January 19, 2005 1:49 PM
To: [redacted] (OGC) (OGA)
Cc: [redacted] (OCA) (FBI)
Subject: RE: sunset

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Great. [redacted] let me know if you need anything else from us. Julie

-----Original Message-----
From: [redacted] (OGC) (OGA)
Sent: Wednesday, January 19, 2005 1:46 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OCA) (FBI)
Subject: sunset

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie:

[redacted] and I just spoke and agreed that we would take out the sublist of USA Patriot Act provisions that will sunset and just refer to them generally [redacted] will send DOJ our comments concerning the significant purpose standard in FISA.

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

X. PATRIOT ACT

A. Legal Changes Accomplished by the Act:

- Information Sharing Increased
- Substantive criminal offense provisions created and/or amended (RICO, Title III, Terrorist statutes)
- Procedural criminal investigative technique provisions amended (Title III, EPCA, Pen Register)
- Amendments to FISA substantive and procedural law provisions (Elsur, Physical Search, Pen Register, Business Records, NSLs)

B. Title III Intelligence Information-Sharing by Criminal Investigators

Section 203: Amends Title III, 18 USC Section 2517 to add subsection (6), to permit disclosure of Title III information when the matter involves foreign intelligence or counterintelligence information "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official . . . to assist the official who is to receive that information in the performance of his official duties."

C. Grand Jury Intelligence- Information Sharing by Criminal Investigators

Section 203: Amends Federal Rule of Criminal Procedures, Rule 6(e)(3)(C) to permit disclosure of Grand Jury information involving foreign intelligence or counterintelligence information "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security information in the performance of official duties."

Requires Notice to the Court of the agencies to which information was disseminated.

D. Intelligence Information-Sharing by Criminal Investigators

Section 905: Requires disclosure of foreign intelligence acquired in criminal investigations to Director of CIA (50 USC 105(B))

Guidelines for implementation issued by Attorney General in late September, 2002

E. Catch-All Intelligence Information-Sharing By Criminal Investigators

Section 203: Establishes that "notwithstanding any other law" it is lawful for criminal investigators to share foreign intelligence or counterintelligence information obtained in the course of a criminal investigation with any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in the performance of official duties.

Please note: INTELLIGENCE INFORMATION-SHARING PROCEDURES

Section 203: Procedural Changes

FBI components intending to disseminate foreign intelligence information to the Intelligence Community, obtained through the use of criminal investigative techniques MUST: 1) Coordinate dissemination through substantive CD or CTD Units at FBIHQ and comply with other DOJ procedures once in place; 2) Comply with the provisions of the Third Agency Rule, if applicable.

Roving FISA Authority

- Section 206: Allows the FISA Court during the issuance of a FISA ELSUR Order to issue a generic order to unspecified carrier where the Court finds that "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means when a target is otherwise [redacted] the Court can direct "other persons [redacted] (S) (S) (S) (S)
- No need to get another order – can serve same order on another new provider
- Similar to roving Title III under 19 USC 2518 (11), (12) – in 2518 (12), for wire and electronic communications, as in roving FISA, need evidence that actions of target "could have effect of thwarting interception from a specified facility."

b1
b2
b7E

Increased FISA Durations

Section 207: Extends the standard duration for several categories of FISA Orders.

- Increased duration of ELSUR and physical search orders on non-USP who are agents of a foreign power, limited to AFPs who are officers or employees of foreign power, or members of group engaged in international terrorism:

- Initial period of authorization - 120 days (instead of 90)
- Renewal for periods of one year

- Increased duration of physical search orders on all other targets from 45 to 90 days.

FISA Pen Register/Trap and Trace Authority Expanded

Section 214: FISA Pen Registers & Trap and Trace Orders

- Changes standard of FISA Pen Register/Trap and Trace court order
- Pre-Patriot Act – standard was relevance plus specific and articulable facts that target was an agent of foreign power
- [redacted] b5 b1
- [redacted] (S)

FISA Business Records Authority Expanded

Section 215: Changes FISA standard to a simple showing of relevance (same standard as Pen Register/ NSLs) , and gives the FISC authority to compel production of "any tangible things, including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation as a USP is not conducted solely upon the basis of activities protected by the First Amendment.

Pre-Patriot Act – could only get business records court order for records from common carriers, public accommodations, vehicle rentals, storage facilities – based on relevance and specific and articulable facts that records related to agent of foreign power.

FISA NSL Authority Expanded

NSLs are issued in FCI/IT investigations to obtain telephone, electronic communications records from telephone companies and ISPs, pursuant to ECPA, Financial Records from financial institutions, pursuant to Right to Financial Privacy Act (RFPA) and information from credit bureaus, pursuant to the Fair Credit Reporting Act (FCRA).

Section 505: The Patriot Act changes the standard predication for the three acts above

and all three types of NSLs to "relevant to an authorized investigation to protect against international terrorism, clandestine intelligence activities," provided investigation of USP not based solely on First Amendment activities and allows the Director to delegate signature authority to SAC level.

Pre-Patriot Act standard – relevance and specific and articulable facts to believe agent of foreign power

Information re: associates or individuals in contact with the subject could be targets on NSLs.

FISA "Primary Purpose" change

The Patriot Act clarifies the "primary purpose" issue in FISA. FISC previously interpreted meaning that foreign intelligence, as opposed to criminal prosecution, had to be primary purpose.

Section 218 changes FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amends FISA to allow that personnel involved in a FISA may consult with law enforcement to coordinate and protect against attacks, terrorism, sabotage, or clandestine intelligence activities, without putting the FISA at risk

XI. INFORMATION SHARING

A. Overview:

Look to: FISA statute, Minimization Procedures, Attorney General Guidelines, 2001 Patriot Act, Attorney General March 6, 2002 Procedures, FISA APPELLATE COURT OPINION DATED NOVEMBER 18, 2002----FISC May 17, 2002 order, and NFIP Manual for information-sharing/dissemination guides

- Special rules apply to FISA material and USP material so need to recognize when information is derived from FISA material, and/or when it concerns USPS
- Also need to keep in mind when information derived from foreign sources or other federal agencies, so that their rules are followed in FBI dissemination of their material (ORCON)
- Need to ensure that recipient follows FBI rules in its dissemination of FBI-derived material

B. Minimization procedures – per FISA Section 101(h)

- Specific procedures adopted by the Attorney General and approved by FISC
- Designed in light of purpose and technique of the particular surveillance
- To minimize acquisition and retention, and prohibit dissemination, of nonpublicly available information concerning unconsenting USP consistent with USG needs to obtain, produce and disseminate FI information
- Per FISA Section 101(h), procedures must require that nonpublicly available USP information which IS NOT FI, cannot be disseminated without USP consent unless identity is necessary to understand FI information or assess its importance
- Per FISA Section 101(h), procedures must allow for dissemination to law enforcement authorities of evidence of crime that has been, is being, or is about to be committed

C. Minimization procedures –PER FISA Section 101(e)

- General rule – USP non-public FISA information can be disseminated without USP consent if information is/reasonably appears to be FI information (section 101(e) (1) and (2) of FISA) or evidence of crime

- Relates to their authorized responsibilities
- Is required by EO 10450
- Is required by statute, EP, interagency agreement

Section 2-50: Disseminate to foreign law enforcement, intelligence and security services when:

- Information is relevant to functions of those agencies
- Dissemination is consistent with U.S. national security interests
- FBI takes into account effect of dissemination on USPS; dissemination of USP information from unconsented physical searches require Attorney General approval
- If dissemination may significantly affect foreign relations, need to coordinate with State Department

G. Patriot Act Information sharing provisions – Intelligence officials to Criminal officials

- Patriot Act (November 2001) – attempt to fix "wall" – promote information sharing
- Title II, Section 218 – FI as "significant purpose" replaces FI as "the purpose" of FISA ("The purpose" language had been interpreted by FISC as "primary" purpose.)
- Title V, Section 504 – federal officers running FISAs to acquire FI can consult with federal LE officers to coordinate efforts to investigate or protect against attack, sabotage, IT, clandestine intelligence activities -- without undermining "significant" purpose Removes fear that consulting with criminal prosecutors will negate FI "purpose" and prevent FISA.

H. Patriot Act - Information sharing provisions –Criminal officials to Intelligence officials II

- Sharing of FI information from GJ or Title III wiretap with Intelligence officials
- Title II, Section 203 amends Federal Rule of Criminal Procedures Rule 6(e), Title III to allow sharing of Title III and GJ information involving foreign intelligence or counter intelligence with other federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent necessary to perform his duty.

- Requires Attorney General to develop procedures for sharing information when USPS involved – not yet promulgated

- Section 203 adds that "notwithstanding any other law," it is lawful for criminal investigators to share FI information obtained in course of a criminal investigation with any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

I. Information Sharing with CIA

- Section 905 – Law Enforcement must disclose FI acquired during course of criminal investigation to Director, CIA

J. Can you use FI/FCI in a Criminal Case?

- Yes, if it was obtained legally and you have authority to disseminate it. But must follow certain procedures established by the Attorney General and approved by FISC designed to assure that FI and FCI investigations are conducted lawfully and to promote effective coordination and performance of DOJ's criminal and CI functions

K. March 6, 2002 Attorney General Intelligence Sharing Procedures for FI/FCI Investigations (Issued by Attorney General but later modified by FISC and later modified by FISA APPELLATE COURT) – Removing Walls

- Attorney General March 6, 2002 Intelligence Sharing Procedures –

- Open file policy - DOJ Criminal Division, OIPR have access to FBI FI/FCI investigative information; AUSAs have access to IT investigative information; FBI duty to keep DOJ Criminal Division and OIPR apprized of FI and FCI investigation information, including FI information and information re crime

- FBI duty to provide DOJ Criminal Division/OIPR LHM in full FI/FCI investigations

- Regular consultations between FBI, DOJ Criminal Division, and OIPR

- FBI duty to keep AUSA apprized of IT investigation information

- FBI duty to provide AUSA LHM in IT cases

- Regular consultations between FBI and AUSAs

[redacted]RMD) (FBI)

From: [redacted]OCA) (FBI) b6
Sent: Wednesday, January 19, 2005 12:55 PM b7C
To: [redacted](OGC) (OGA)
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: Expiring Laws

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179DMH/BAW 05-cv-0845

UNCLASSIFIED
NON-RECORD

[redacted] I'm a little confused by NSLB's input as it relates the Patriot Act §224. You've listed specific sections that if permitted to expire will adversely impact FBI operations. Based on my review, you've listed all of the provisions that are scheduled to sunset (and some that aren't - see §224 re §203 - only (b) will sunset). If we have something to say about specifically how the sunset of each provision will adversely impact FBI ops, that would be great - but if we don't I'm not sure why we want to list them. Please let me know or give me a call. Thanks,

[redacted]
Special Counsel
Office of Congressional Affairs
[redacted]

-----Original Message-----
From: [redacted](OGC) (OGA) b6
Sent: Wednesday, January 19, 2005 11:25 AM b7C
To: [redacted](OCA) (FBI); [redacted](OCA) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: Expiring Laws

UNCLASSIFIED
NON-RECORD

[redacted]

Here is NSLB's response. I reached out to [redacted]or comments ILU may have, but haven't heard back.

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, January 18, 2005 5:34 PM
To: [redacted](OGC) (OGA)
Subject: FW: Expiring Laws

UNCLASSIFIED
NON-RECORD b6
b7C

[redacted] I forwarded this to [redacted] but seem to recall he has a drs. appt tomorrow. Obviously, there are some laws which we care about on this list. Can we cut and paste from our wishlist to forward our comments by the deadline? Julie

-----Original Message-----
From: Caproni, Valerie E. (OGC) (FBI)
Sent: Tuesday, January 18, 2005 8:51 AM
To: KELLEY, PATRICK W. (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); GULYASSY, ANNE M. (OGC)

(FBI)
Subject: FW: Expiring Laws

UNCLASSIFIED
NON-RECORD

please check for your areas of interest.

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Friday, January 14, 2005 9:35 AM
To: [redacted] (OGC) (FBI); Caproni, Valerie E. (OGC) (FBI)
Cc: [redacted] OCA) (FBI); [redacted] (OCA)(FBI)
Subject: Expiring Laws

b6
b7C

UNCLASSIFIED
NON-RECORD

One of the things that DOJ does each January is to assist OMB in compiling a list of laws that are scheduled to expire (e.g., grant programs that are enacted for a set number of years). Please take a look at the attached list and advise if you have any additions, deletions, or corrections.

In the chart "a/a" means "appropriation authorization"; "b/l" means "basic law".

b6
b7C

Please E-mail your comments to [redacted] with a cc to [redacted] **Your comments should be prepared in Microsoft Word format** which is suitable for dissemination to DOJ and to congressional staff. Please send these comments to the OCA contact person as an attachment to your E-mail. If you have additional comments which are not suitable for dissemination, please include them in the body of your E-mail separate and apart from the attachment. If your division is not taking a position and has no comments, please send an E-mail to the OCA contact person stating such.

DEADLINE 11:00 am 1-19-04. We appreciate your attention to this matter.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (RMD) (FBI)

From: [redacted] (OGC) (OGA)
Sent: Wednesday, February 23, 2005 12:02 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

yes.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, February 23, 2005 11:41 AM
To: [redacted] (OGC) (OGA)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

Did you work on this?

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179DMH/BAW 05-cv-0845

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III [redacted]
Unclassified Fax: [redacted]
Secure Fax [redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, February 23, 2005 9:46 AM
To: [redacted] (OGC) (FBI)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report
Importance: High

UNCLASSIFIED
NON-RECORD

[redacted]

I don't think so. But this is OBE anyway, because the deadline was yesterday.

[redacted]

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, February 23, 2005 8:36 AM
To: [redacted] (OGC) (FBI)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

You commented right?

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, February 21, 2005 2:51 PM
To [redacted] (OGC) (FBI)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

Did I already forward this to you? Haven't we already commented on this once? Julie

b6 -----Original Message-----
b7C **From:** [redacted] OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

[redacted] nd Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcmte on Terrorism and is meant to:
1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments to [redacted] ext. [redacted] by **9:00 am, Tuesday, 2/22/05**.

Thanks for your assistance.

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (RMD) (FBI)

From: [redacted] OGC) (FBI)
Sent: Wednesday, February 23, 2005 1:58 PM
To: [redacted] (OGC) (OGA)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

Please send Julie and I an e-mail that you did this.

Thanks

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179DMH/baw 05-cv-0845

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III: [redacted]
Unclassified Fax: [redacted]
Secure Fax: [redacted]

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (OGA)
Sent: Wednesday, February 23, 2005 12:02 PM
To: [redacted] (OGC) (FBI)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

yes.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, February 23, 2005 11:41 AM
To: [redacted] (OGC) (OGA)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

Did you work on this?

[redacted]

National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III: [redacted]
Unclassified Fax: [redacted]
Secure Fax: [redacted]

b2
b6
b7C

-----Original Message-----
From [redacted] (OGC) (FBI) b6
Sent: Wednesday, February 23, 2005 9:46 AM b7C
To: [redacted] OGC) (FBI)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report
Importance: High

UNCLASSIFIED
NON-RECORD

[redacted]

I don't think so. But this is OBE anyway, because the deadline was yesterday.

[redacted] b6 b7C

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Wednesday, February 23, 2005 8:36 AM
To [redacted] (OGC) (FBI)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

You commented right?

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, February 21, 2005 2:51 PM b6
To [redacted] (OGC) (FBI) b7C
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

Did I already forward this to you? Haven't we already commented on this once? Julie
-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
b6 **Cc** [redacted] (OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
b7C **Subject:** Request for Comments re: PATRIOT Act Sunsets Report

UNCLASSIFIED
NON-RECORD

[redacted] and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcmte on Terrorism and is meant to:
1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect

the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments t[redacted] ext. [redacted] by **9:00 am, Tuesday, 2/22/05**.

Thanks for your assistance.

[redacted]

Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] RMD) (FBI)

From: [redacted] OGC) (OGA)
Sent: Wednesday, January 19, 2005 1:46 PM
To: THOMAS, JULIE F. (OGC) (FBI) b6
Cc: [redacted] (OCA) (FBI) b7C
Subject: sunset

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie:

[redacted] and I just spoke and agreed that we would take out the sublist of USA Patriot Act provisions that will sunset and just refer to them generally. [redacted] will send DOJ our comments concerning the significant purpose standard in FISA.

b6
b7C

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-09-2005 BY 65179DMH/BAW 05-cv-0845

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 1
Page 23 ~ Duplicate

ORIGINAL EC NOTIFICATIONS NOT ON ACS...

Litigation #05-CV-0845

SIGNED OUT
READY TO BO
CLOSED ADMIN.

Litigation #05-CV-0845

ORIGINAL
EC NOT
UPLOADED

Precedence: ROUTINE Date: 10/21/2004

To: Director's Office Attn: OPR
Counterintelligence Attn: AD
Washington Field Attn: SAC
CDC

From: General Counsel
NSLB/CILU/Room 7975
Contact: [redacted] ext. [redacted] b2 b6 b7C

Approved By: Thomas Julie
[redacted] b6

Drafted By: [redacted] b7C

Case ID #: ~~(S)~~ 278-HQ-C1229736-VIO (Pending)
(U) ~~(S)~~ 105A-WF-223252 (Pending)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD MATTER
IOB 2004-77

Synopsis: ~~(S)~~ (U) The Office of the General Counsel (OGC) considers that this matter must be reported to the Intelligence Oversight Board (IOB) and to the Office of Professional Responsibility (OPR). OGC will prepare an appropriate cover letter and a memorandum to the IOB. Our analysis follows. b1 b2 b6 b7A b7C b7E

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

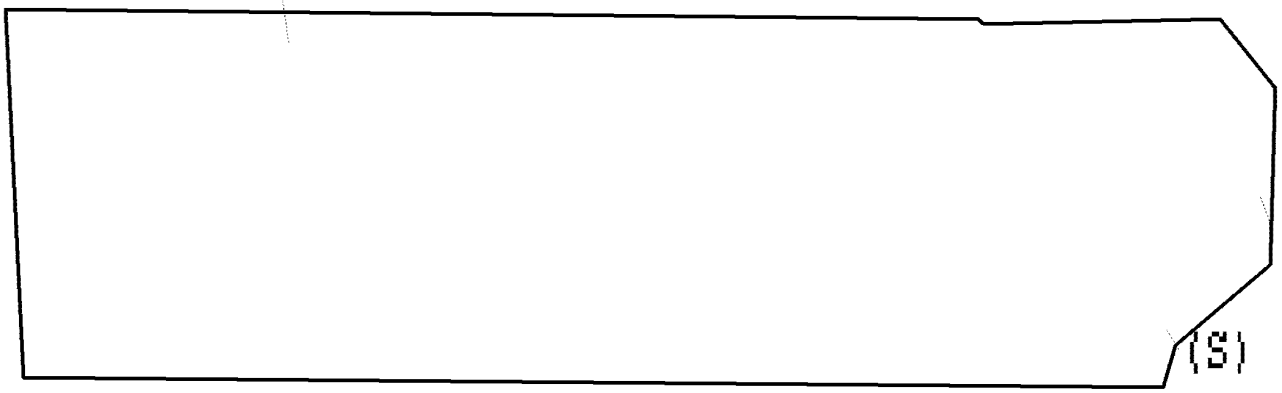
DATE: 08-15-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-15-2030

Details: ~~(S)~~ [redacted] (S)

[redacted] (S)

[redacted] (S)

~~(S)~~ [redacted] (S) b1 b2 b6 b7A b7C b7E



b1
b2
b6
b7A
b7C
b7E

(U) The Right to Financial Privacy Act (RFPA), Title 12, United States Code, Section 3401 et seq. (12 USC 3401 et seq.) states in 3402 that "ïe´xcept as provided by section 3403(c) or (d), 3413, or 3414 of this title, no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution . . .."

(U) 12 USC 3414 provides in part:

(a)(1) Nothing in this chapter (except sections 3415, 3417, 3418, and 3421 of this title) shall apply to the production and disclosure of financial records pursuant to requests from--

(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities; or
(B) . . .

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

(U) Section 2-17 of the National Foreign Intelligence Program Manual (NFIPM) lists the FBI officials who can request financial records under the foregoing section of RFPA. According to section 2-17 of the NFIPM, such requests must be made by an Assistant Special Agent in Charge or a more senior official.

(U) 12 USC 3417 provides for civil liability of an agency or department of the United States that obtains financial records or information in violation of the RFPA. The same section deals with "disciplinary action for wilful or intentional violation" of these RFPA provisions by agents or employees of the government.

b6
b7C

(S) In this instance, the conduct of SA [redacted] was wilful and intentional, even though she did not realize that she had acted in contravention of the RFPA and Bureau policy. It (U)

should also be noted that SA [redacted] was at the time a probationary agent. Inasmuch as her actions nevertheless amount to "intelligence activities that . . . may be unlawful or contrary to Executive order or Presidential directive" they are reportable to the Intelligence Oversight Board (IOB) under the terms of section 2.4 of Executive Order 12863. OGC will therefore prepare a cover letter and a memorandum to report this matter to the IOB and to advise that it has been referred to the Office of Professional Responsibility. (U) b6 b7C

LEAD(s):

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 2: (Action)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) Please read and clear.

Set Lead 3: (Action)

WASHINGTON FIELD

AT WASHINGTON, DC

(U) For action deemed appropriate.

~~SECRET~~

BY COURIER

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure entitled, "Intelligence Oversight Board (IOB) Matter, IOB 2004-77." (U)

The enclosure sets forth details of investigative activity which the FBI has determined may have been contrary to the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

1 - Ms. Thomas
1 - [redacted]
1 -

1 - IOB Library
1 - 278-HQ-C1229736-VIO

b6
b7C

~~Derived from: G-3~~
~~Declassify on: X25-1~~

~~SECRET~~
~~SECRET~~
-2-

General Brent Scowcroft (USAF Retired)

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience.

Sincerely,

Julie Thomas
Deputy General Counsel

Enclosure

1 - The Honorable John D. Ashcroft
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

b7A

(S) Investigation of this IOB matter has determined that [redacted] (S)

(S) Such information is relevant in national security investigations of this type.
However, the proper method for obtaining bank records is through a National Security Letter
under Title 12, United States Code, Section 3414(a)(1)(A). Access to financial records by
government authorities through means not provided by law is prohibited under Title 12, United
States Code, Section 3402. (U)

(S) [redacted]

[redacted] (U)

b7A

(U) This matter has been referred to the FBI's Office of Professional Responsibility for
such action as may be appropriate.

~~Derived from: G-3~~
~~Declassify on: X25-1~~

~~SECRET~~

IP FAILED TO FILE A 90 DAY LHM + ANNUAL LHM THAT SHOULD HAVE BEEN PREPARED & FORWARDED BY 8/17/03 WAS NOT REC'D UNTIL 10/20/03. A LHM WAS PREPARED ON 7/18/03, BUT NOT UPLOADED.

NO TEXT...

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/29/2004

To: Indianapolis **Attn:** SAC

Director's Office **Attn:** Office of Professional Responsibility (OPR)

Counterterrorism **Attn:** A/AD

From: General Counsel
Counterterrorism Law Unit II
Contact: [redacted] b2 b6 b7C

Approved By: Curran John F [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: 278-HQ-C1229736-VIO -411
IP 278-0

DECLASSIFIED BY 65179/DMH/JW/05-CV-0845
ON 08-10-2005

Title: (U) INTELLIGENCE OVERSIGHT BOARD MATTER(IOB)
IOB 2003 148

Synopsis: ~~(S)~~ It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB) and to the Office of Professional Responsibility (OPR), FBIHQ. OGC will prepare a cover letter and a memorandum to report this matter to the IOB. Our analysis follows.(U)

(U) ~~G-3~~ ~~X1~~ ~~Derived From :~~ ~~Declassify On:~~

Reference: 315T-IP-92406

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in Corel WordPerfect.

~~SECRET~~

OIG/DOJ Review: Vm DATE: 4/8/05
FBI INVEST: M OIG/DOJ INVEST.:
OPR UC INITIALS:

To: Counterterrorism Division From: General Counsel
Re: ~~(S)~~ 278-HQ-C1229736-VIO, 01/28/2004

Details: ~~(S)~~ As discussed in the electronic communication (EC)[1] dated November 3, 2003, FBI Indianapolis prepared and forwarded a letterhead memorandum (LHM) for the full investigation (FI) on subject [redacted] a U.S. person, on April 17, 2002. [redacted] is a "United States person" as that term is used in the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG).[2] The initiation and continuation of the FI required FBI Indianapolis and the Headquarters' substantive unit to comply with the requirements of Executive Order (EO) 12863 and the FCIG. In this regard, [redacted] became the subject of a FBI full investigation on April 17, 2002, in the Indianapolis Division. The required 90-day LHM was not filed. Additionally, the annual LHM that should have been prepared and forwarded to FBIHQ on or before April 17, 2003, was not received until October 20, 2003. It should be noted that the LHM was prepared on or about July 18, 2003, but for unknown reasons, it was not uploaded into ACS. In October of 2003, when FBI Indianapolis was notified that the annual LHM had not be received at FBIHQ, the same was forwarded. On November 3, 2003, FBI Indianapolis advised FBIHQ and the Office of the General Counsel that they had failed to comply with the 90-day and annual reporting requirements.

b6
b7C

(U) Because the subject of the investigation was (and remains) a "United States person" as that term is used in Section 101(i) of the Foreign Intelligence Surveillance Act of 1978 (FISA) and Section II.W of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG)[3], continuation of the

---

[1] ~~(S)~~ EC from FBI Indianapolis to OGC, dated 11/03/2003 and titled "Potential IOB Matter." (U)

[2] ~~(S)~~ A "United States person" is defined in Section II.W. of the FCIG as "an individual who is ....[a] United States citizen . . . or . . . [b] a permanent resident alien . . . ." (U)

[3] ~~(S)~~ A "United States person" is defined in Section 101(i) of the Foreign Intelligence Surveillance Act (FISA)(codified at 50 U.S.C. § 1801 et seq.) as "a citizen of the United States [or] an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . ." See also section II.W of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. (U)

investigation required that Indianapolis and the Headquarters' substantive unit comply with the reporting requirements of Executive Order 12863 and the FCIG. FBI Indianapolis failed to submit the 90-day LHM, due on or about July 17, 2002, and the annual LHM, due on or about April 17, 2003, to the National Security Law Branch (NSLB), OGC, for submission to the Office of Intelligence Policy and Review (OIPR), Department of Justice (DOJ), as required by the FCIG. As a result of these errors, OIPR was not advised of the status of the ongoing investigation for approximately eighteen months.(U)

(U) Section 2.4 of Executive Order (E.O.) 12863, dated September 13, 1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive." This language was adopted verbatim from E.O. 12334, dated December 4, 1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a provision of the FCIG, or other guidelines or regulations approved by the Attorney General in accordance with E.O. 12333, dated 12/04/1981, if such provision was designed in full or in part to ensure the protection of the individual rights of U.S. persons. Violations of provisions that are essentially administrative in nature need not be reported to the IOB. The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

(S) Section IX of the FCIG sets forth rules governing the reporting, dissemination, and retention of information concerning foreign counterintelligence and international terrorism investigations. Section IX.C provides in pertinent part that: (U)

> Each full investigation of any U.S. person shall be reported within ninety (90) days of initiation to the Office of Intelligence Policy and Review, setting forth the basis for undertaking the investigation. **The FBI shall furnish to the Attorney General or a designee a summary of each investigation at**

> **the end of each year the investigation continues**, including specific information on any requests for assistance made by the FBI to foreign law enforcement, intelligence or security agencies. (Emphasis added.)

(S) Section IX.C is intended to regulate the timely reporting of FBI full investigations on U.S. persons to the OIPR. As such, it was written to include both administrative and "rights protection" components. The annual reporting requirements of Section IX.C is purely administrative in nature, while the oversight exercised by the OIPR in reviewing the required reporting ensures the protection of individual rights. As a general rule, delinquent annual LHMs are considered to be violations of an administrative nature when they are submitted to the NSLB within 90 days of their original due date. These administrative violations are placed in the control file for periodic review by the Counsel to the IOB. When an LHM is not submitted at all, or is submitted later than 90 days from its original due date, the facts and circumstances of that particular case must be examined to determine whether the failure or substantial delay in submitting the LHM precluded meaningful oversight and review by the OIPR. If the OIPR was precluded from conducting such oversight and review, then the matter must be reported to the IOB. (U)

(S) As previously discussed, in this instance, OIPR was not updated of the status of this ongoing investigation involving a U.S. person for approximately fifteen months. This delayed reporting clearly precluded OIPR from exercising its responsibility for oversight and approval of an ongoing foreign counterintelligence investigation of a U.S. person, which is contrary to the requirements of the FCIG. (U)

(S) Based upon the above analysis, and consistent the reporting requirements of Section 2.4 of E.O. 12863, OGC will prepare a cover letter and an LHM to report this matter to the IOB. That correspondence will also advise the IOB that this matter will be referred to the FBI's Office of Professional Responsibility. The latter is a matter within the cognizance of the IMU. (U)

To: Counterterrorism Division From: General Counsel
Re: (U) (S) 278-HQ-C1229736-VIO, 01/28/2004

LEAD(s):

Set Lead 1: (Discretionary)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) (S) For action deemed appropriate.

Set Lead 2: (Discretionary)

COUNTERTERRORISM

(U) (S) For action deemed appropriate.

b6
b7C

1 - [redacted]
1 - NSLB Library

NO TEXT
AVAILABLE
FOR ORIGINAL
EC REPORTING
[redacted]

IOB S705.WPD

(01/26/1998)

~~SECRET~~

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/10/2005

To: Director's Office
Counterintelligence

Attn: OPR
Attn: UC [redacted]
Attn: SSA [redacted]

From: Office of the General Counsel
National Security Law Branch/CILU/Room 7975
Contact: [redacted]

b2
b6
b7C

Approved By: Thomas Julie F [redacted]

b6
b7C

Drafted By: [redacted]

Case ID #: ~~(S)~~ (U) ~~278-HQ-C1229736-VIO~~
~~(S)~~ 278-HQ-1416655

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD
IOB 2003-29

Please handle
ensure OPR
load restored

DECLASSIFIED BY 65179/DMH/JW/05-CV-0845
ON 08-10-2005

Synopsis: ~~(S)~~ (U) It is the opinion of the Office of General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB). OGC will prepare and deliver the necessary correspondence to the IOB.

~~(S)~~ (U) ~~**Derived from : G-3**~~
~~**Declassify On: X25-1**~~

Reference: ~~(S)~~ (U) 278-HQ-1416655 Serial 2

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect.

Details: (U) ~~(S)~~ As discussed in the electronic communication (EC)[1], on 02/01/02 New York Office (NYO) submitted a letterhead

---

(U) ~~(S)~~ EC from Inspection to the General Counsel and the Director's Office, dated 04/01/03 and titled "UC [redacted];] SSA [redacted];] Counterintelligence Division [;] IOB 2003 29." (INSD EC)

~~SECRET~~

b6
b7C

memorandum (LHM) requesting initiation of a full investigation (FI), on [redacted] who was a "United States person" as that term is used in the then existing Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG).[2] The initiation and continuation of the FI required that NYO and the Headquarters' substantive unit comply with the requirements of Executive Order 12863 and the FCIG. In this regard, NYO submitted its initial 90-day LHM to the Headquarters' substantive unit (former NS-3A, currently CD-3A) via electronic communication (EC) dated 02/01/02. On 01/31/03, NYO submitted its annual LHM. Subsequent to this submission, on 02/14/03, the National Security Law Unit (NSLU) advised that its records did not show the receipt of the initial 90-day LHM. The Headquarters' substantive unit was unable to verify the submission of the 90-day LHM to NSLU or Office of Intelligence Policy and Review (OIPR).[3] The reason why the 90-day LHM was not received by NSLU or OIPR remains unexplained. However, the consequence is clear: NYO's 90-day LHM was not forwarded to OIPR as required.(U)

b6
b7C

(U) Section 2.4 of Executive Order (EO) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive Order or Presidential Directive. This language was adopted verbatim from EO 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a

---

[2] (U) (S) A "United States person" is defined in Section II.W. of the FCIG as "an individual who is. . . [a] United States citizen . . . or . . . [b] a permanent resident alien . . . ." On 10/31/03, the FCIG were superseded by the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). However, because this potential error occurred while the FCIG were in effect, the potential error is analyzed within the context of the then existing FCIG.

[3] (U) INSD EC.

To: Counterintelligence Division From: General Counsel
Re: ~~(S)~~ 278-HQ-C1229736 , 02/10/2005
(U)

provision of the FCIG, or other guidelines or regulations approved by the Attorney General in accordance with EO 12333, dated 12/04/1981, if such provisions were specifically intended to ensure the protection of the individual rights of U.S. persons. Violations of provisions that are essentially administrative in nature need not be reported to the IOB. The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

(U) ~~(S)~~ Section IX of the FCIG set forth rules governing the reporting of information concerning foreign counterintelligence and international terrorism investigations. Section IX.C provided in pertinent part that:

> Each full investigation of any U.S. person **shall be reported within ninety (90) days of initiation** to the Office of Intelligence Policy and Review, setting forth the basis for undertaking the investigation. The FBI shall furnish to the Attorney General or a designee **a summary of each investigation at the end of each year the investigation continues**, including specific information on any requests for assistance made by the FBI to foreign law enforcement, intelligence or security agencies. (Emphasis added.)

(U) ~~(S)~~ Section IX.C was intended to regulate the timely reporting of FBI full investigations on U.S. persons to the OIPR. As such, it was written to include both administrative and "rights protection" components. The 90-day and annual reporting requirements of Section IX.C were purely administrative in nature, while the oversight exercised by the OIPR in reviewing the required reporting ensured the protection of individual rights. As a general rule, delinquent annual or 90-day LHMs were considered to be violations of an administrative nature when they were submitted to the NSLU within 90 days of their original due date. These administrative violations were placed in a control file for periodic review by the Counsel to the IOB. When an LHM was not submitted at all, or was submitted later than 90 days

To: Counterintelligence Division From: General Counsel
Re: (U) (S) 278-HQ-C1229736 , 02/10/2005

from its original due date, the facts and circumstances of that particular case were examined to determine whether the failure or substantial delay in submitting the LHM precluded meaningful oversight and review by the OIPR. If OIPR was precluded from conducting such oversight and review then the matter was required to be reported to the IOB. (U)

(S) As previously discussed, the reason why NYO's 90-day LHM was not received by the NSLU from the Headquarters substantive unit remains unexplained. As a result of the lack of submission, OIPR was not advised of the status of this ongoing investigation involving a U.S. person for over a year. This delayed reporting clearly precluded OIPR from exercising its oversight and review of an ongoing foreign counterintelligence investigation of a U.S. person, and was contrary to the requirements of the then existing FCIG. Consequently, in accordance with the reporting requirements of Section 2.4 of E.O. 12863, OGC will prepare correspondence to report this matter. (U)

LEAD (s):

Set Lead 1: (Action)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) For action deemed appropriate.

Set Lead 2: (Action)

DIRECTOR'S OFFICE

AT OPR, DC

(U) For action deemed appropriate.

CC: Ms. Thomas
[redacted] b6 b7C
IOB Library

To: Counterintelligence Division From: General Counsel
Re: ~~(S)~~ 278-HQ-C1229736 , 02/10/2005
(U)

♦♦

BY COURIER

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure, entitled Intelligence Oversight Board (IOB) Matter, Counterintelligence Division, IOB Matter 2003-29. (U)

This enclosure sets forth details of investigative activity which the FBI has determined was conducted contrary to the then existing Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations and/or laws, Executive Orders, or Presidential

Directives which govern FBI foreign counterintelligence and international terrorism investigations. This matter has also been referred to our Office of Professional Responsibility for a determination of whether any administrative action is warranted. (U)

Enclosure

1 - Ms. Thomas
1 - [redacted]
1 - [redacted]
1 - IOB Library
1 - 278-HQ-C1229736-VIO

b6
b7C

~~UNCLASSIFIED WHEN~~
~~DETACHED FROM~~
~~CLASSIFIED ENCLOSURE~~

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience. (U)

Sincerely,

Julie F. Thomas
Deputy General Counsel

1 - The Honorable Alberto Gonzales
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice

Room 6150

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
COUNTERINTELLIGENCE DIVISION

2003-29 (U)

(U)

(S) Investigation of this IOB matter has determined that on February 1, 2002, the New York Office of the Federal Bureau of Investigation ("FBI") requested initiation of a full investigation (FI) on [redacted] who was a United States person as that term was used in the then existing Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG).[1] Thus, the initiation and continuation of the FI required that the New York Office and the Headquarters' substantive unit comply with the requirements of Executive Order 12863 and the FCIG. The New York Office submitted a letterhead memorandum (LHM) to the Headquarters' substantive unit (former NS-3A, currently CD-3A) requesting the

b6
b7C

initiation of this FI. However, the Headquarters' substantive unit did not forward this LHM to the National Security Law Unit nor to the Office of Intelligence Policy and Review. As a consequence of the error, for over a year, OIPR was precluded from exercising oversight and control of this ongoing investigation, which was contrary to the requirements of Section IX.C of the then existing FCIG.

~~Derived from : G-3~~
~~Declassify on: X25-1~~

~~SECRET~~

FOOTNOTES

(U)

ï1´: ~~(S)~~ A United States person is defined in Section II.W of the FCIG as an individual who is. . . ïa´ United States citizen . . . or . . . ïb´ a permanent resident alien . . . . On 10/31/03, the FCIG were superseded by the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). However, because this potential error occurred while the FCIG were in effect, the potential error is analyzed within the context of the then existing FCIG.

UC [redacted] cw

SSA [redacted]

IOB MATTER

263-0-

b6

b7C

OIG/DOJ Review: [redacted] DATE: 12/22/04

FBI INVEST.: M OIG/DOJ INVEST.: _____

OPR UC INITIALS: _____

b6

b7C

[redacted] 1

2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-10-2005 BY 65179/DMH/JW/05-CV-0845

This is a reportable IOB matter, but in the OPR context I view her actions as deficient in the performance area (new Agent didn't understand/know Rules) This should go into the Complaint d/b as IOB issue + Performance issue

NOT UPLOADED
105A-WF-223252
SERIAL # 104

(Rev. 01-31-2003)

Lead assigned to [redacted] SSA in ACS Clear lead.

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

Precedence: ROUTINE Date: 10/21/2004

To: Director's Office Attn: OPR
Counterintelligence Attn: AD
Washington Field Attn: SAC
CDC

From: General Counsel
NSLB/CILU/Room 7975
Contact: [redacted] ext. [redacted]

b2
b6
b7C

Approved By: Thomas Julie
[redacted]

Drafted By: [redacted]

Case ID #: ~~(S)~~ 278-HQ-C1229736-VIO (Pending) — 600
(U) ~~(S)~~ 105A-WF-223252 (Pending)

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD MATTER
IOB 2004-77

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Synopsis: ~~(S)~~ (U) The Office of the General Counsel (OGC) considers that this matter must be reported to the Intelligence Oversight Board (IOB) and to the Office of Professional Responsibility (OPR). OGC will prepare an appropriate cover letter and a memorandum to the IOB. Our analysis follows.

b1
b2
b6
b7A
b7C
b7E

~~(S)~~ ~~Derived From~~ : G-3
~~Declassify On~~: X1

DATE: 08-15-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-15-2030

Details: ~~(S)~~ [redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] ~~(S)~~

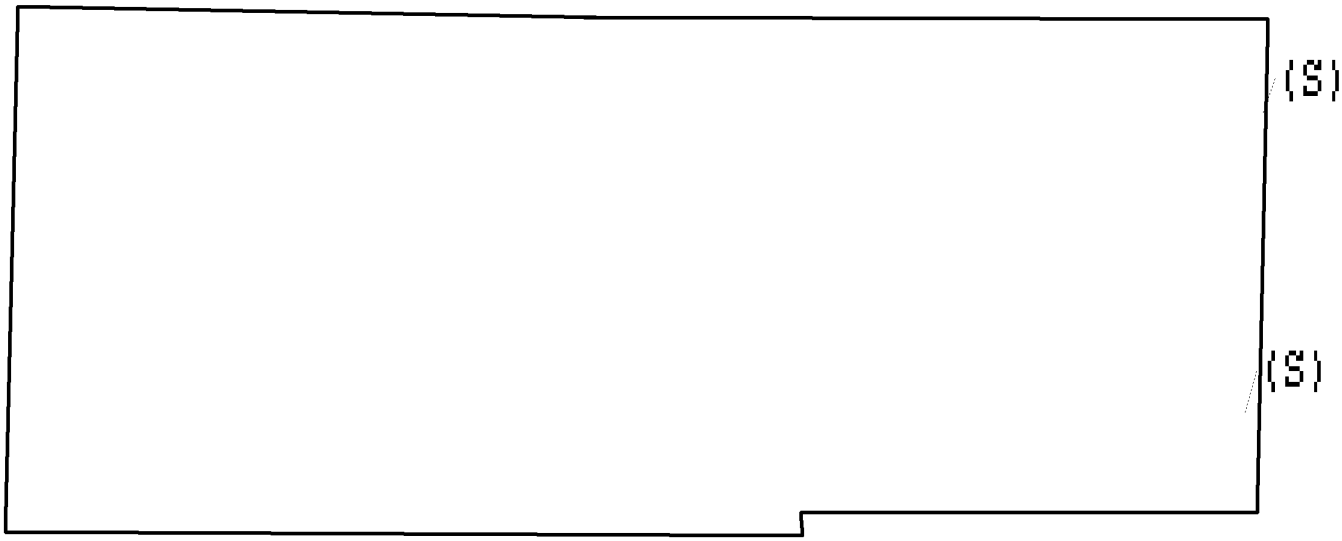
b1
b2
b6
b7A
b7C
b7E

~~SECRET~~

A.SAC Heimbach DOB
SSA
SA [redacted] Eff. 11/3/04

b5
b6
b7A
b7C

To: Director's Office From: General Counsel
Re: (U) (S) 278-HQ-C1229737-VIO, 10/21/2004



(U) The Right to Financial Privacy Act (RFPA), Title 12, United States Code, Section 3401 et seq. (12 USC § 3401 et seq.) states in §3402 that "[e]xcept as provided by section 3403(c) or (d), 3413, or 3414 of this title, no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution . . .."

(U) 12 USC §3414 provides in part:

(a)(1) Nothing in this chapter (except sections 3415, 3417, 3418, and 3421 of this title) shall apply to the production and disclosure of financial records pursuant to requests from--

(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities; or
(B) . . .

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

(U) Section 2-17 of the National Foreign Intelligence Program Manual (NFIPM) lists the FBI officials who can request

financial records under the foregoing section of RFPA. According to section 2-17 of the NFIPM, such requests must be made by an Assistant Special Agent in Charge or a more senior official (U)

(U) 12 USC §3417 provides for civil liability of an agency or department of the United States that obtains financial records or information in violation of the RFPA. The same section deals with "disciplinary action for wilful or intentional violation" of these RFPA provisions by agents or employees of the government.

(U) (~~S~~) In this instance, the conduct of SA [redacted] was wilful and intentional, even though she did not realize that she had acted in contravention of the RFPA and Bureau policy. It should also be noted that SA [redacted] was at the time a probationary agent. Inasmuch as her actions nevertheless amount to "intelligence activities that . . . may be unlawful or contrary to Executive order or Presidential directive" they are reportable to the Intelligence Oversight Board (IOB) under the terms of section 2.4 of Executive Order 12863. OGC will therefore prepare a cover letter and a memorandum to report this matter to the IOB and to advise that it has been referred to the Office of Professional Responsibility.

b6
b7C

To: Director's Office From: General Counsel
Re: ~~(S)~~ (U) 278-HQ-C1229737-VIO, 10/21/2004

LEAD(s):

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 2: (Action)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) Please read and clear.

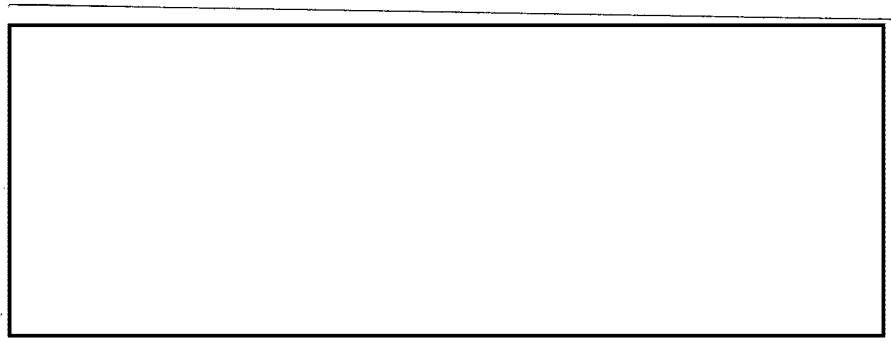
Set Lead 3: (Action)

WASHINGTON FIELD

AT WASHINGTON, DC

(U) For action deemed appropriate.

♦♦



b7A

(NO TEXT) AVAIL FOR SERIAL 41

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 1/22/2004

To: Counterterrorism **Attn:** AD John S. Pistole
A/SSA [redacted]
ITOS I, CONUS II, Team 8
Office of Professional Responsibility (OPR)
SSA [redacted]
SA [redacted]

Director's Office

Kansas City

b6
b7C

From: General Counsel
National Security Law Branch/Room 7975
Contact: [redacted] Ext. [redacted]

b2
b6
b7C

Approved By: Kelley Patrick W
[redacted]

b6
b7C

Drafted By: [redacted]

300

Case ID #: ~~(S)~~ (U) 278-HQ-C1229736-VIO (Pending)

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD MATTER 2003-153

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Synopsis: (U) ~~(S)~~ It is the opinion of the Office of the General Counsel (OGC) that the late submission of a 90-day letterhead memorandum (LHM) must be reported to the Intelligence Oversight Board (IOB). OGC will prepare and deliver the required correspondence to the IOB. Our analysis follows.

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

DATE: 08-12-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-12-2030

Reference: (U) ~~(S)~~ 315B-KC-84651 Serial 41

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect 8.0.

~~SECRET~~

OIG/DOJ Review: Vom DATE: 4/18/05
FBI INVEST.: M OIG/DOJ INVEST.: _____
OPR UC INITIALS: _____

To: Counterterrorism From: General Counsel
Re: (U) ~~(S)~~ 278-HQ-C1229736-VIO, 1/22/2004

Details: ~~(S)~~ As noted in the referenced electronic communication (EC),

(S)

b1
b6
b7A
b7C

(U) Section 2.4 of Executive Order (E.O.) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive." This language was adopted verbatim from E.O. 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a provision of the FCIG, or other guidelines or regulations approved by the Attorney General in accordance with E.O. 12333, dated 12/04/1981, if such provision was designed to ensure the protection of the individual rights of U.S. persons. Violations

[1] ~~(S)~~ A "United States person" is defined in Section 101(i) of the Foreign Intelligence Surveillance Act (FISA)(codified at 50 U.S.C. § 1801 et seq.) as "a citizen of the United States [or] an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . ." See also Section II.W of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counter-intelligence Investigations.

of provisions that are essentially administrative in nature need not be reported to the IOB. The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

~~(S)~~ Section IX of the FCIG sets forth the rules governing the reporting, dissemination, and retention of information concerning foreign counterintelligence and international terrorism investigations. Section IX.C provides in pertinent part: (U)

> Each full investigation of any U.S. person **shall be reported within ninety (90) days of initiation** to the Office of Intelligence Policy and Review, setting forth the basis for undertaking the investigation. **The FBI shall furnish to the Attorney General or a designee a summary of each investigation at the end of each year the investigation continues,** including specific information on any requests for assistance made by the FBI to foreign law enforcement, intelligence or security agencies.

(Emphasis added, classification marking omitted).

(U) ~~(S)~~ Section IX.C of the FCIG is intended to regulate the timely reporting of FBI full investigations on U.S. persons to the Office of Intelligence Policy and Review (OIPR), Department of Justice. As such, it was written to include both administrative and "rights protection" components. The 90-day and annual reporting requirements of Section IX.C are purely administrative in nature, while the oversight exercised by the OIPR in reviewing the required reporting ensures the protection of individual rights. As a general rule, delinquent annual or 90-day LHMs are considered to be violations of an administrative nature when they are submitted to the NSLU within 90 days of their original due date. These administrative violations are placed in the control file for periodic review by the Counsel to the IOB. However, when a LHM is not submitted at all, or is submitted later than 90 days from its original due date, the facts and circumstances of that particular case must be examined to determine whether the failure or substantial delay in submitting the LHM precluded meaningful oversight and review

To: Counterterrorism From: General Counsel
Re: (U) ~~(S)~~ 278-HQ-C1229736-VIO, 1/22/2004

b7A

by the OIPR. If the OIPR was precluded from conducting such oversight and review, then the matter must be reported to the IOB.

(U) ~~(S)~~ [redacted] This is a violation of Section IX.C of the FCIG which must be reported to the IOB

(U) ~~(S)~~ In accordance with the reporting requirements of Section 2.4 of E.O. 12863, OGC will prepare the correspondence required to report this matter to the IOB.

To: Counterterrorism From: General Counsel
Re: (U)(~~S~~) 278-HQ-C1229736-VIO, 1/22/2004

LEAD (s)

Set Lead 1:

COUNTERTERRORISM DIVISION

AT WASHINGTON, DC

(U) For action deemed appropriate.

Set Lead 2: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 3: (Action)

KANSAS CITY

AT KANSAS

(U) For action deemed appropriate.

1 - [redacted]
♦♦

b6
b7C

FEDERAL BUREAU OF INVESTIGATION HEADQUARTERS (FBIHQ)
IOB MATTER 2004-21 (U)

(S) By electronic communication (EC) dated February 11, 2004, the Counterintelligence Division reported a possible IOB error [redacted] b1 b2 b7A b7E In this regard, the Counterintelligence Division reported that [redacted] (S) (S)

(S) [redacted] b1 b2 b7A b7E (S)

[redacted] (S) b1 b2 b7A b7E (S) Thus, in accordance with the reporting requirements of Section 2.4 of E.O. 12863, this mistake must be reported to the IOB.

(S) ~~Derived From : G-3~~
~~Declassify On: X25-1~~

NO TEXT
ACCESS DENIED

Precedence: ROUTINE
Date: 10/22/2004

To: Counterintelligence
Attn: Section Chief

Directors Office
Attn: Office of Professional Responsibility

SAN FRANCISCO
Attn: SAC

From: General Counsel
National Security Affairs/Room 7975
Contact: [redacted] [redacted]
b2 b6 b7C

Approved By: Thomas Julie F
[redacted]
b6

Drafted By: [redacted] :rss
b7C

Case ID #: ~~(S)~~ (U) 278-HQ-1425173

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD (IOB)
IOB MATTER 2003-56

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Synopsis: (U) ~~(S)~~ It is the opinion of the Office of the General Counsel (OGC) that this matter need not be reported to the Intelligence Oversight Board (IOB), but, rather, that a record of this decision should be maintained in the investigative control file for review by the Counsel to the IOB.

(U) ~~Derived from : G-3~~
~~Declassify On: X1~~

DATE: 08-11-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C) (D)
DECLASSIFY ON: 08-11-2030

Reference: (U) ~~(S)~~ 278-HQ-1425173
[redacted]
b2 b7D

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect 8.

Details: (U) Referenced electronic communications from the Inspection Division (ID) to OGC, National Security Law Branch (NSLB), dated May 28, 2003, advised OGC of a possible IOB violation involving actions exceeding the authorized scope of otherwise permitted activity OGC has reviewed the facts of the captioned matter and has determined that reporting to the IOB is not warranted. Our analysis follows.

~~(S)~~ As set forth in the referenced ECs, San Francisco Division was conducting a Full Field NFIP Investigation of a
b1
[redacted] (S)

(S)

SA SA under the supervision of SSA

b1
b6
b7C
b7D

No NSL had been issued.

(S)

Upon discovery of the mistake, an appropriate NSL was prepared covering the period 01/10/01-04/30/03.

(U) Also following discovery of this mistake, additional training and advice was provided to San Francisco investigative personnel regarding the proper use of NSL and the restrictions pertaining to b7D without a NSL.

(U) (S) Section 2-56 of the National Foreign Intelligence Program Manual requires OGC to determine whether the facts related above must be reported to the IOB. Based on the analysis set forth below, it is OGC's determination that they need not be in this instance.

(U) Section 2.4 of Executive Order (E.O.) 12863, dated September 13, 1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

(S) Title 18, United States Code, Section 2709, Counterintelligence access to Telephone Toll and Transactional Records states that:

> (b) Required certification. --The Director of the Federal Bureau of Investigation, or his designee . . . may-
>
> (1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director . . .certifies in writing to the wire or electronic communication service

provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation ...

(U) In the case of a US Person, such failure to comply would likely constitute an IOB violation. In the instant case, however, the subject of the investigation was not a US Person but rather a [redacted] (S) b1 As such, the sole determination we must make is whether the FBI's failure to conform to its internal administrative requirements -i.e., the National Foreign Intelligence Program Manual (NFIPM)- is reportable as a matter of policy, to the IOB.

(S) As previously discussed, in this instance, probationary Special Agent [redacted] met on numerous occasions with his asset. [redacted] (S) Both SA [redacted] and his supervisor were operating under the mistaken belief that the information provided was covered under an existing FISA. Upon learning of the mistake, a NSL was retrospectively issued to cover the period in question. It is clear that the error committed did not impinge upon the individual rights of a US Person. Although the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigation (FCIG) have been modified as of October 31, 2003, the underlying principal remains the same, and consequently, because only violations of the FCIG which are designed to safeguard the rights of U.S. persons are required to be reported to the IOB, it is our opinion that this matter need not be reported to the IOB. Consistent with our prior opinions, a record of this decision should be maintained in the control file for future review by Counsel to the IOB. (U)

b1
b6
b7C
b7D

Lead(s):

Set Lead 1: (Action)

COUNTERINTELLIGENCE DIVISION

AT WASHINGTON, DC

(U) For action deemed appropriate.

Set Lead 2: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 3: (Action)

SAN FRANCISCO

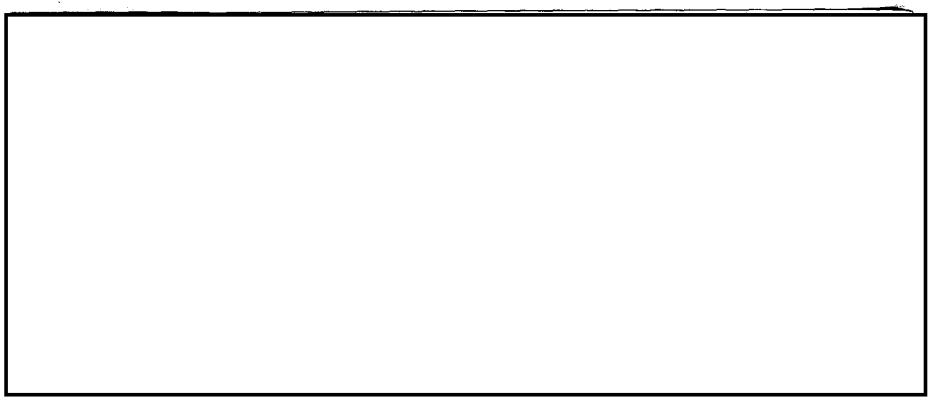
AT SAN FRANCISCO, CALIFORNIA

(U) For action deemed appropriate.

1 - [redacted] b6 b7C

FOOTNOTES (U)

ï1´:(S) OGC EC to INSD, dated May 28, 1999 and titled SSA [redacted]; SA [redacted]; Washington Field Officeï; IOB Matter 97-15. b6 b7C



NO TEXT (NOT UPLOADED)

b7A

(NO TEXT)

(01/26/1998)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 11/17/2003

To: Springfield
Director's Office

Attn: SAC, CDC
Office of Professional
Responsibility

From: General Counsel
National Security Law Branch (NSLB)/Room 7974
Contact: [redacted] Ext. [redacted] b2 b6 b7C

Approved By: Kelley Patrick W
[redacted]

DECLASSIFIED BY 65179/DMH/JW/05-CV-0845
ON 08-11-2005

Drafted By: [redacted] b6 b7C

Case ID #: ~~(S)~~ (U) 278-HQ-1416800 -3

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD MATTER
IOB MATTER 2003-31

Synopsis: ~~(S)~~ It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB). OGC will prepare a cover letter and a memorandum to report this matter to the IOB. (U)

(U) ~~Derived From : G-3~~
~~Declassify On: X25-1~~

Reference: ~~(S)~~ 278-HQ-C1229736-VIO Serial 81 (U)

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect 8.0.

Details: (U) An electronic communication (EC) from the Inspection Division (INSD) to OGC, dated 04/01/2003, requested that OGC review the facts of the referenced EC to determine whether the matter described should be reported to the Intelligence Oversight Board (IOB). In our opinion, it should. Our analysis follows.

~~SECRET~~

OIG/DOJ Review: Vom DATE: 4/18/05
FBI INVEST.: MG OIG/DOJ INVEST.:
OPR UC INITIALS:

b7A

To: Springfield From: General Counsel
Re: (U) (S) 278-HQ-1416800, 11/17/2003

(U) (S) As discussed in the referenced EC, [redacted]

[redacted]

(U) (S) Because the unknown subject was (and remains) a "United States person", continuation of the investigation required that Springfield comply with the requirements of Executive Order 12863 and the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG).[3]

(U) Section 2.4 of Executive Order (E.O.) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive." This language was adopted verbatim from E.O. 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a provision of the FCIG, or other guidelines or

b6
b7C

[1] (U) Related per telephone call from SA [redacted] to AGC [redacted] on 05/16/03.

[2] (U) (S) See Section III.C.2(a) of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations.

[3] (U) At the time of this investigation, the FCIG were in effect.

regulations approved by the Attorney General, in accordance with E.O. 12333, dated 12/04/1981, if such provision was designed in full or in part to ensure the protection of the individual rights of a U.S. person. Violations of provisions that are essentially administrative in nature need not be reported to the IOB. The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

(U) (S) Section IX of the FCIG sets forth the rules governing the reporting, dissemination, and retention of information concerning foreign counterintelligence and international terrorism investigations. Section IX.C provides in pertinent part:

> Each full investigation of any U.S. person **shall be reported within ninety (90) days of initiation** to the Office of Intelligence Policy and Review, setting forth the basis for undertaking the investigation. The FBI shall furnish to the Attorney General or a designee **a summary of each investigation at the end of each year the investigation continues**, including specific information on any requests for assistance made by the FBI to foreign law enforcement, intelligence or security agencies.

(Emphasis added, classification marking omitted).

(U) (S) Section IX.C of the FCIG is intended to regulate the timely reporting of FBI full investigations on U.S. persons to the OIPR. As such, it was designed to include both administrative and "rights protection" components. The 90-day and annual reporting time requirements of Section IX.C are purely administrative in nature, while the oversight exercised by the OIPR in reviewing the required reporting ensures the protection of individual rights. As a general rule, delinquent annual or 90-day LHMs are considered to be violations of an administrative nature when they are submitted to the NSLU within 90 days of their original due date. These administrative violations are placed in the control file for periodic review by the Counsel to the IOB. However, when an LHM is not submitted at all, or is submitted later than 90-days from its original due date, the facts and circumstances of that particular case must be examined to determine whether the failure or substantial delay in submitting the LHM precluded meaningful oversight and review by the OIPR. If the OIPR

was precluded from conducting such oversight and review, then the matter must be reported to the IOB.

(U) (S)

[redacted] b7A

(U) (S) In accordance with the reporting requirements of Section 2.4 of E.O. 12863, OGC will prepare a cover letter and a memorandum for the Deputy General Counsel to report this matter to the IOB.

To: Springfield From: General Counsel
Re: (U) ~~(S)~~ 278-HQ-1416800, 11/17/2003

LEAD (s)

Set Lead 1: (Action)

SPRINGFIELD DIVISION

AT QUAD CITY RA

(U) For action consistent with this opinion.

Set Lead 2: (Action)

DIRECTOR'S OFFICE

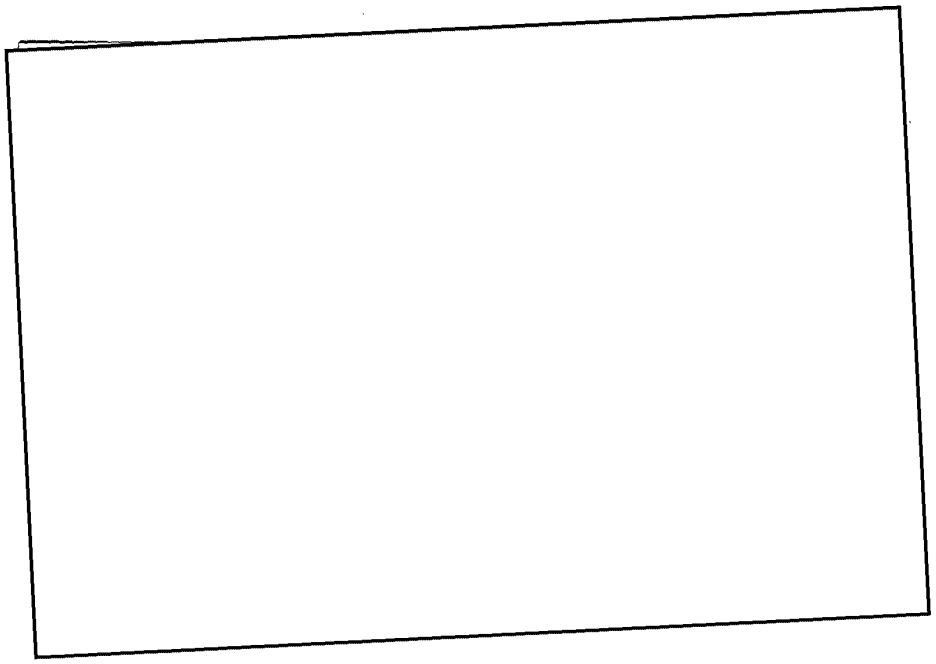
AT OPR FO, DC

(U) For action deemed appropriate.

1 - [redacted]

b6
b7C

♦♦



b7A
b6
b7C

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 12/05/2003

To: Pittsburgh **Attn:** SAC Kenneth T. McCabe
CDC Jeffrey B. Killeen

Director's Office **Attn:** Office of Professional Responsibility

From: Office of the General Counsel
National Security Law Branch/CILU/Room #7975
Contact: (A) UC [redacted] b2 b6 b7C

Approved By: Kelley Patrick W b6 b7C
Curran John F
[redacted] b7C

DECLASSIFIED BY 65179/DMH/JW/05-CV-0845
ON 08-11-2005

Drafted By: [redacted] vim

Case ID #: ~~(S)~~ (U) 278-HQ-1425174 -3

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD (IOB)
IOB MATTER 2003-57

Synopsis: ~~(U)~~ ~~(S)~~ It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB). OGC will prepare a cover letter and a letterhead memorandum to report this matter to the IOB. Our analysis follows.

(U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: ~~(U)~~ ~~(S)~~ 278-HQ-1425174 Serial 2

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect.

Details: ~~(S)~~ (U) As discussed in the referenced electronic communication (EC), on 03/30/2000, [redacted] b7A

~~SECRET~~

OIG/DOJ Review: Vam DATE: 4/18/05
FBI INVEST.: (M) OIG/DOJ INVEST.:
OPR UC INITIALS:

To: Pittsburgh From: Office of the General Counsel
Re: ~~(S)~~ (U) 278-HQ-1425174, 12/05/2003

[redacted] b7A

[redacted] U)

(U) Section 2.4 of EO 12863, dated 09/13/1993, mandates that Inspectors General and General Counsels of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB concerning intelligence activities that they have reason to believe may be unlawful or contrary to an EO or Presidential Directive. This language was adopted verbatim from EO 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a provision of the FCIG, or other guidelines or regulations approved by the Attorney General in accordance with EO 12333, dated 12/04/1981, if such provisions were specifically intended to ensure the protection of the individual rights of U.S. persons. Violations of provisions that are essentially administrative in nature need not be reported to the IOB.

(U)~~(S)~~ A "United States person" is defined in Section 101(i) of the Foreign Intelligence Surveillance Act (FISA) (codified at 50 U.S.C. § 1801 et seq.) as "a citizen of the United States [or] an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . ." See also Section II.W of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations.

[2] (U) Since that time, the Attorney General has issued new guidelines for FBI National Security Investigations and Foreign Intelligence Collection, dated October 31, 2003. However, since the actions occurred prior to the issuance of the new guidelines, the old guidelines are cited herein.

The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

(U) (S) With regard to the continuation of an FBI PI, Section III.B.6 of the FCIG provides in pertinent part that:

> Preliminary inquiries shall be completed within 120 days of the date of initiation. The Office of origin SAC may personally authorize extensions of a preliminary inquiry for a period of not more than 90 days up to a total of one year when justified by facts or information obtained during the course of the inquiry. . . . FBI Headquarters may authorize additional extensions for periods of not more than 90 days on the same basis. All extensions shall be in writing and include the justification for the extension.
>
> (Emphasis added.)

(U) (S) Although this provision of the Attorney General Guidelines is primarily administrative in nature, it was designed in part to protect the rights of U.S. persons by limiting the length of time that the FBI can conduct a PI without periodic oversight by the proper authorities. Pursuant to the aforementioned agreement between the FBI and IOB, PI overruns are not reported to the IOB if they are both inadvertent and de minimus in time. To determine whether a possible violation of the FCIG is "inadvertent" and "de minimus in time," all the facts relevant to the incident must be considered.

(U) (S) [redacted] b7A [redacted] This activity was, thus, inconsistent with the requirements of the FCIG. Consequently, in accordance with the reporting requirements of Section 2.4 of EO 12863, OGC will prepare a cover letter and an LHM to report this matter to the IOB. As a mitigating circumstance, it is recognized that the source provided valuable information during the overrun relative to a counterterrorism matter.

To: Pittsburgh From: Office of the General Counsel
Re (U) ~~(S)~~ 278-HQ-1425174, 12/05/2003

To: Pittsburgh From: Office of the General Counsel
Re: ~~(S)~~ (U) 278-HQ-1425174, 12/05/2003

LEAD(s):

Set Lead 1: (Info)

PITTSBURGH

AT PITTSBURGH

(U) For information.

Set Lead 2: (Discretionary)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

CC: SAC Pittsburgh
Mr. Kelley
Mr. Curran
[redacted] b6 b7C
IOB Library

♦♦

DN OPENED A PI ON 6/13/02. INITIAL PI EXPIRED 10/10/02, BUT NOT FORMALLY EXTENDED UNTIL 1/11/03. BETWEEN EXPIRATION OF INITIAL PI AND THE FORMAL EXTENSION 1/11/03 INV. WAS CONDUCTED BY DN.

- APPEARS TO BE INADVERTENT w/ROP

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 1/16/04

To: Director's Office **Attn:** OPR

Counterterrorism **Attn:** AD

Denver **Attn:** SAC
CDC

From: General Counsel
National Security Law Branch/Room 7975
Contact: [redacted] ext. [redacted]

b2
b6
b7C

Approved By: Curran John F
Lammert Elaine N

b6
b7C

Drafted By: [redacted] 351

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Case ID #: ~~(S)~~ (U) 278-HQ-C1229736-VIO (Pending)

Title: ~~(S)~~ (U) POSSIBLE INTELLIGENCE OVERSIGHT BOARD MATTER
2003-142

Synopsis: ~~(S)~~ (U) It is the opinion of the Office of General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB) and to the Office of Professional Responsibility (OPR), FBIHQ. OGC will prepare and deliver the required correspondence to the IOB. Our analysis follows.

~~Derived From : G-3~~
~~Declassify : X1~~

DATE: 08-15-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-15-2030

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the documents in Corel Wordperfect.

OIG/DOJ Review: Vom DATE: 4/18/05 ~~SECRET~~
FBI INVEST.: M OIG/DOJ INVEST.:
OPR UC INITIALS:

To: Director's Office From: General Counsel
Re: (S) 278-HQ-C1229736-VIO, 1/16/04

(U) (S)

b1
b6
b7C

Details: (S) As noted in the electronic communication (EC) referenced below,[1] on June 13, 2002, the Denver Division initiated a preliminary inquiry (PI) on [redacted] who is a "United States person" as that term is used in Section 101(i) of the Foreign Intelligence Surveillance Act of 1978 (FISA).[2] Thus, of the PI required that Denver comply with the requirements of the Attorney General Guidelines for FBI Foreign Intelligence Collections and Foreign Counterintelligence Investigations (FCIG). The initial PI expired on October 10, 2002, but was not formally extended by Denver on January 11, 2003. This extension expired on April 10, 2003. Between the expiration of the initial PI on October 10, 2002 and the extension on January 11, 2003, Denver conducted an investigation with respect to [redacted] specifically, on December 20, 2002, a source was contacted for information [redacted] within the Denver Division.[3] (S)

(U) Section 2.4 of Executive Order (E.O.) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsels of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive." This language was adopted verbatim from E.O. 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), the language has been

---

1 (S) (U) EC from the Denver Division to INSD, dated 10/20/03 and titled "SSA [redacted] SA [redacted] Denver Division [;] IOB [;]. Hereinafter cited as "Denver EC." b6 b7C

2 (S) (U) A "United States person" is defined in Section 101(i) of the Foreign Intelligence Surveillance Act (FISA) (codified at 50 U.S.C. § 1801 et seq.) as "a citizen of the United States [or] an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act)...." See also Section II.W of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations.

3 Denver EC.

interpreted to mandate the reporting of any violation of a provision of the FCIG, or other guidelines or regulations approved by the Attorney General in accordance with E.O. 12333, dated 12/04/1981, if such provision was designed to ensure the protection of the individual rights of U.S. persons. Violations of provisions that are essentially administrative in nature need not be reported to the IOB. The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

(S) (U) With regard to the continuation of an FBI preliminary inquiry, Section III.B.6 of the FCIG[4] provides, in pertinent part that

> Preliminary inquiries shall be completed within 120 days of the date of initiation. The Office of origin SAC may personally authorize extensions of a preliminary inquiry for a period of not more than 90 days up to a total of one year when justified by facts or information obtained during the course of the inquiry.... FBI Headquarters may authorize additional extensions for periods of not more than 90 days on the same basis. All extensions shall be in writing and include the justification for the extension.

(Emphasis added, classification marking omitted).

Although this provision of the Attorney General Guidelines is primarily administrative in nature, it was designed in part to protect the rights of U.S. persons by limiting the length of time that the FBI can conduct a PI without periodic oversight by the proper authorities. Pursuant to the aforementioned agreement between the FBI and IOB, PI overruns are not reported to the IOB if they are both inadvertent and de minimis in time. To determine whether a possible violation of the FCIG is "inadvertent" and "de minimis in time," all the facts relevant to the incident must be considered.

[4]At the time of this investigation, the FCIG were in effect.

To: Director's Office From: General Counsel
Re: ~~(S)~~ (U) 278-HQ-C1229736-VIO, 1/16/04

~~(S)~~ (U) In the instant matter, while the PI overrun between the expiration date and the date of the renewal appears to have been inadvertent, it was not de minimis in time; investigative activity continued for three months before the renewal, during which time a source was contacted. Consequently, based on the above analysis, and in accordance with the reporting requirements of Section 2.4 of E.O. 12863, OGC will prepare the correspondence required to report this matter to the IOB.

LEAD(s):

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 2: (Action)

COUNTERTERRORISM

AT WASHINGTON, DC

(U) For Action Deemed Appropriate.

Set Lead 3: (Action)

Denver

(U) For action deemed appropriate.

1 -Mr. Curran
1 -Ms. Lammert
1 [redacted]
1 -IOB Library

b6
b7C

♦♦

To: Director's Office From: General Counsel
Re: ~~(S)~~ (U) 278-HQ-C1229736-VIO, 1/16/04

NIPC WAS CONDUCTING A MONITERING OF E-MAIL. ~~THIS~~ 3 E-MAIL PROVIDERS FORWARDED DATA AFTER EXPIRATION OF THE FISC ORDER.

UPON REVIEW OF THIS INFO NIPC DETERMINED THE MISTAKE & IMMEDIATELY NOTIFIED THE PROVIDERS

- ERROR BY THE PROVIDERS NOT UPLOADED

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/15/2004

To: Director's Office **Attn:** OPR
Counterterrorism **Attn:** AD

From: General Counsel
Counter Terrorism Law Unit I / Rm. 7975
Contact: [redacted]

Approved By: Curran John F
Lammert Elaine N

Drafted By: [redacted] :asc

Case ID #: ~~(S)~~ (U) 278-HQ-C1229736-VIO -333

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD MATTER
IOB 2003 131

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Synopsis: ~~(S)~~ (U) It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB) and to the Office of Professional Responsibility (OPR), FBIHQ. OGC will prepare a cover letter and an enclosure for the Deputy General Counsel to report this matter to the IOB.

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X25-1~~

DATE: 08-15-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-15-2030

Reference: ~~(S)~~ (U) 278-HQ-C1229736-VIO Serial 112

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in Corel WordPerfect.

Details: (U) Referenced communication from CTD to OGC, dated 07/3/02 (received 10/7/03), requested that OGC review the facts of the captioned matter to determine whether it must be reported to the IOB. In our opinion, it must. Our analysis follows.

~~(S)~~ As discussed in the referenced electronic communication (EC), on 6/20/02, at approximately 4:30 pm EDT, the Special Technologies and Applications Unit (STAU) of the National Infrastructure Protection Center (NIPC) was conducting a

~~SECRET~~

OIG/DOJ Review: Vaney DATE: 4/18/05
FBI INVEST.: [redacted] OIG/DOJ INVEST.: _____
OPR UC INITIALS: _____

To: Director's Office From: General Counsel
Re: (S) (U) 278-HQ-C1229736-VIO Serial 112, 01/05/2004

b1
b2
b6
b7C
b7E

voluntary audit of Foreign Intelligence Surveillance Court (FISC)

[redacted] (S)

(S) Upon review of the information received by STAU, it was determined that the

[redacted] (S)

b1
b2
b7E

(U) Section 2.4 of Executive Order (E.O.) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB all information "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive." This language was adopted verbatim from E.O. 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board.

(U) Title 18, United States Code, Section 2511(2)(f) states that the procedures contained in the FISA and Title III of the 1968 Omnibus Crime Control Act (as amended by the Electronic Communications Privacy Act) "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted." Additionally, Section 2.5 of E.O. 12333 provides that, "[e]lectronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order." Under Title 50, United States Code, Section 1802(b), the FISC is authorized to grant an order approving the electronic surveillance of a foreign power or an agent of a foreign power for the purposes of obtaining foreign

---

(U) (S) It cannot be determined from the referenced EC whether [redacted] If that has not yet been done, it should be done now.

b2
b6
b7C
b7E

intelligence information. Under the pertinent FISA definition, the term electronic surveillance means, "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(2).

(U) ~~(S)~~ In this instance, it is clear that as a consequence of an error on the part of the communications carriers, the FBI (unintentionally) conducted an electronic surveillance which was unauthorized. The carrier's error must be reported to the IOB. OGC will prepare an appropriate cover letter and an enclosure for the Deputy General Counsel to report this matter to the IOB.

To: Director's Office From: General Counsel
Re: (S) (U) 278-HQ-C1229736-VIO Serial 112, 01/05/2004

LEAD(s):

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 2: (Info)

COUNTERTERRORISM

AT WASHINGTON, DC

(U) Please read and clear.

CC: Mr. Curran
Ms. Lammert
[redacted] b6 b7C
IOB Library

♦♦

VAULT LOCATE
ORIGINAL REQUESTING
EC

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 01/28/2004

To: Detroit **Attn:** SAC

Director's Office **Attn:** Office of Professional Responsibility (OPR)

Counterterrorism Division **Attn:** A/AD

From: General Counsel
Counterterrorism Law Unit II
Contact: [redacted] b2 b6 b7C

Approved By: Curran John F
[redacted] b6

Drafted By: [redacted] b7C

Case ID #: 278-HQ-C1229736-VIO 335
66-DE-A5102

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Title: (U) INTELLIGENCE OVERSIGHT BOARD MATTER(IOB)
IOB 2003 145

Synopsis: ~~(S)~~ (U) It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB) and to the Office of Professional Responsibility (OPR), FBIHQ. OGC will prepare a cover letter and a memorandum to report this matter to the IOB. Our analysis follows.

(U) ~~G-3~~ ~~X1~~ ~~Derived From :~~ ~~Declassify On:~~

DATE: 08-15-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-15-2030

Reference: 315G-DE-92951, Serial 140, 141

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in Corel WordPerfect.

~~SECRET~~

OIG/DOJ Review: Vany DATE: 4/18/05
FBI INVEST.: (M) OIG/DOJ INVEST.:
OPR UC INITIALS:

To: Counterterrorism Division From: General Counsel
Re: (S) 278-HQ-C1229736-VIO, 01/28/2004 (U)

Details: (U) (S) As discussed in the electronic communication (EC)[1] on October 31, 2003, FBI Detroit prepared and forwarded a letterhead memorandum (LHM) for the full investigation (FI) on (S) subject [redacted] a U.S. person, on May 11, 1998. [redacted] is a "United States person" as that term is used in the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG).[2] The initiation and continuation of the FI required FBI Detroit and the Headquarters' substantive unit to comply with the requirements of Executive Order (EO) 12863 and the FCIG. In this regard, (S) [redacted] became the subject of a FBI full investigation on May 11, 1998, in the New York Division. The New York Division prepared and submitted the FBI HQ annual LHMs on May 23, 2000 and May 1, 2001. The next required annual LHM should have been filed with FBIHQ in May, 2002. The investigation was transferred to FBI Detroit on October 17, 2001. On October 31, 2003, FBI Detroit advised FBIHQ and the Office of the General Counsel that they had failed to comply with the annual reporting requirements.

b1
b6
b7C

(U) Because the subject of the investigation was (and remains) a "United States person" as that term is used in Section 101(i) of the Foreign Intelligence Surveillance Act of 1978 (FISA) and Section II.W of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG)[3], continuation of the investigation required that Detroit and the Headquarters' substantive unit comply with the reporting requirements of Executive Order 12863 and the FCIG. Due to delay in forwarding a hard copy of the investigation to FBI Detroit following notification of the investigation being transferred, and an

---

(U) [1] (S) EC from FBI Detroit to INSD and OGC, dated 10/31/2003 and titled "Intelligence Oversight Board (IOB) Matter."

(U) [2] (S) A "United States person" is defined in Section II.W. of the FCIG as "an individual who is ....[a] United States citizen . . . or . . . [b] a permanent resident alien . . . ."

(U) [3] (S) A "United States person" is defined in Section 101(i) of the Foreign Intelligence Surveillance Act (FISA)(codified at 50 U.S.C. § 1801 et seq.) as "a citizen of the United States [or] an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . ." See also section II.W of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations.

To: Counterterrorism Division From: General Counsel
Re (U) (S) 278-HQ-C1229736-VIO, 01/28/2004

administrative order, Detroit failed to submit the third annual letterhead memorandum (LHM), due on or about May 2, 2002, to the National Security Law Unit (NSLU), OGC, for submission to the Office of Intelligence Policy and Review (OIPR), Department of Justice (DOJ), as required by the FCIG. As a result of the error, OIPR was not advised of the status of the ongoing investigation for approximately fifteen months. (U)

(U) Section 2.4 of Executive Order (E.O.) 12863, dated September 13, 1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive." This language was adopted verbatim from E.O. 12334, dated December 4, 1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a provision of the FCIG, or other guidelines or regulations approved by the Attorney General in accordance with E.O. 12333, dated 12/04/1981, if such provision was designed in full or in part to ensure the protection of the individual rights of U.S. persons. Violations of provisions that are essentially administrative in nature need not be reported to the IOB. The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

(U) (S) Section IX of the FCIG sets forth rules governing the reporting, dissemination, and retention of information concerning foreign counterintelligence and international terrorism investigations. Section IX.C provides in pertinent part that:

> Each full investigation of any U.S. person shall be reported within ninety (90) days of initiation to the Office of Intelligence Policy and Review, setting forth the basis for undertaking the investigation. **The FBI shall furnish to the Attorney General or a designee a summary of each investigation at the end of each year the investigation continues**, including specific information on

> any requests for assistance made by the FBI to foreign law enforcement, intelligence or security agencies. (Emphasis added.)

(U) (S) Section IX.C is intended to regulate the timely reporting of FBI full investigations on U.S. persons to the OIPR. As such, it was written to include both administrative and "rights protection" components. The annual reporting requirements of Section IX.C is purely administrative in nature, while the oversight exercised by the OIPR in reviewing the required reporting ensures the protection of individual rights. As a general rule, delinquent annual LHMs are considered to be violations of an administrative nature when they are submitted to the NSLB within 90 days of their original due date. These administrative violations are placed in the control file for periodic review by the Counsel to the IOB. When an LHM is not submitted at all, or is submitted later than 90 days from its original due date, the facts and circumstances of that particular case must be examined to determine whether the failure or substantial delay in submitting the LHM precluded meaningful oversight and review by the OIPR. If the OIPR was precluded from conducting such oversight and review, then the matter must be reported to the IOB.

(U) (S) As previously discussed, in this instance, OIPR was not updated of the status of this ongoing investigation involving a U.S. person for approximately fifteen months. This delayed reporting clearly precluded OIPR from exercising its responsibility for oversight and approval of an ongoing foreign counterintelligence investigation of a U.S. person, which is contrary to the requirements of the FCIG.

(U) (S) Based upon the above analysis, and consistent the reporting requirements of Section 2.4 of E.O. 12863, OGC will prepare a cover letter and an LHM to report this matter to the IOB. That correspondence will also advise the IOB that this matter will be referred to the FBI's Office of Professional Responsibility. The latter is a matter within the cognizance of the IMU.

To: Counterterrorism Division From: General Counsel
Re: (S) 278-HQ-C1229736-VIO, 01/28/2004
(U)

LEAD(s):

Set Lead 1: (Discretionary)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) (S) For action deemed appropriate.

Set Lead 2: (Discretionary)

COUNTERTERRORISM

(S) For action deemed appropriate.
(U)

b6
b7C

1 - [redacted]
1 - NSLB Library

BY COURIER

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

Dear General Scowcroft:

Enclosed for your information is a self-explanatory memorandum, entitled "Intelligence Oversight Board (IOB) Matter, IOB 2003 145." (U)

This memorandum sets forth details of investigative activity which the FBI has determined was conducted contrary to the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

Enclosure

1 - [redacted]
1 - 278-HQ-C1229736-VIO

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~UNCLASSIFIED WHEN~~
~~DETACHED FROM~~
~~CLASSIFIED ENCLOSURE~~

DATE: 08-15-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-15-2030

~~Classified by: 39645, NSA/OGC~~
~~Reason: 1.5(c)~~

Declassify on: X1

SECRET

General Brent Scowcroft (USAF Retired)

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience.

Sincerely,

Patrick W. Kelley
Deputy General Counsel

1 - The Honorable John D. Ashcroft
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. H. Marshall Jarrett
Counsel, Office of Professional Responsibility
U.S. Department of Justice
Room 4304

1 - Mr. James Baker
Counsel for Intelligence Policy, OIPR
U.S. Department of Justice

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
IOB 2003 145 (U)

(S)

Investigation of this IOB matter has determined that, on May 11, 1998, the New York Field Office of the Federal Bureau of Investigation ("FBI") requested initiation of a full investigation (IT) o[redacted] who was a "United States person" as that term is used in the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). Thus the initiation and continuation of the IT required FBI New York and the Headquarters substantive unit to comply with the requirements of Executive Order 12863 and the FCIG. FBI New York submitted its initial 90-day letterhead memorandum and two subsequent annual memoranda in a timely fashion. However, after the investigation was transferred to FBI Detroit, the annual memorandum was filed approximately fifteen months later than required. As a result of the delinquent LHM, OIPR was not properly advised of the initiation of the FI in accordance with Section IX.C of the FCIG. This delayed reporting clearly precluded OIPR from exercising its responsibility for oversight and review of an ongoing foreign counterintelligence investigation of a U.S. person, contrary to the requirements of the FCIG. This matter has been referred to the FBI's Office of Professional Responsibility for review and action deemed appropriate.

(S)

b1
b6
b7C

~~Derived from: G-3~~
~~Declassify on: X-1~~

NEEDS ORIGINAL EC REPORTING IOB FROM CI TO OGC

Precedence: ROUTINE Date: 02/16/2005

To: Counterintelligence Attn: AD David W. Szady

Inspection Attn: Internal Investigations Section

From: Office of the General Counsel
National Security Law Branch/CILU/Room 7975
Contact: [redacted] b2 b6 b7C

Approved By: Thomas Julie F [redacted]

Classification per OGA letter dated 08-16-2005

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

Drafted By: [redacted]

Case ID #: ~~(S)~~ (U) 278-HQ-C1229736-VIO

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD MATTER 2004-21

Synopsis: ~~(S)~~ (U) It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB). OGC will prepare and deliver the necessary correspondence to the IOB. b6 b7C

~~(S)~~ (U) ~~Derived From : G-3~~ ~~Declassify On: X25-1~~
DATE: 08-12-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-12-2030

Details: ~~(S)~~ By electronic communication (EC) dated February 11, 2004, the Counterintelligence Division reported a possible IOB error in conjunction with [redacted] In this regard, the Counterintelligence Division reported that [redacted]

[redacted] (S)

[redacted] (S) b1 b2 b7A b7E

[redacted] (S)

[redacted] (S)

[redacted] (S)

(U) Section 2.4 of Executive Order (E.O.) 12863, dated September 13, 1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB all information concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive. Exec. Order No. 12863, 58 Fed. Reg. 48441 (Sept. 13, 1993). This language was adopted from E.O. 12334, dated December 4, 1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB).

(U) By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a provision of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, or other guidelines or regulations approved by the Attorney General in accordance with E.O. 12333, dated December 4, 1981, if such provisions were specifically intended to ensure the protection of the individual rights of U.S. persons.

(U) Under Title 50, United States Code, Section 1822, the FISC is authorized to grant an order approving the physical search of a foreign power or an agent of a foreign power for the purposes of obtaining foreign intelligence information. Under the pertinent FISA definition, the term "physical search" means, any physical intrusion within the United States into premises or property . . . that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. 50 U.S.C. 1801(f)(2).

b1
b2
b7A
b7E

[redacted] (S)

(U) Further, under section 2.4 of E.O. 12333, only the FBI had the authority to conduct an unconsented physical search of [redacted] Section 2.4 of E.O. 12333 provides in pertinent part that:

b2
b7A
b7E

Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as . . . unconsented physical searches . . . unless they are in accordance with procedures established by the head of the agency and approved by the Attorney General. Such procedures

shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

. . .

(b) Unconsented physical searches in the United States by agencies other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes . . .; and

[redacted] (S) b1

Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981) (emphasis added).

(S) As provided in section 2.4 of E.O. 12333, while the FBI had the authority to conduct an unconsented physical search of

[redacted] (S) b1 b2 b7A b7E

Thus, in accordance with the reporting requirements of Section 2.4 of E.O. 12863, this mistake must be reported to the IOB. OGC will prepare an appropriate cover letter and an enclosure for the Deputy General Counsel to report this matter to the IOB.

LEAD(s):

Set Lead 1: (Action)

INSPECTION

AT WASHINGTON, DC

(U) For action deemed appropriated.

Set Lead 2: (Action)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(S) If it has not already been accomplished, ensure that [redacted] (S)

b1
b2
b7A
b7E

CC: Ms. Thomas
[redacted]
IOB Library

b6
b7C

FOOTNOTES

[redacted] (S)

Thus, the New York Division will not be notified of this IOB matter.

b1
b2
b7A
b7E

BY COURIER

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, NW
Washington, D.C. 20503

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure, entitled Intelligence Oversight Board (IOB) Matter 2004-21."

This enclosure sets forth details of investigative activity which the FBI has determined was conducted contrary to the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. This matter has also been referred to our Internal Investigations Section, Inspection Division, for a determination of whether any administrative action is warranted. (U)

Enclosure

1 - [redacted]
1 - 278-HQ-C1229736-VIO

b6
b7C

~~UNCLASSIFIED WHEN DETACHED FROM CLASSIFIED ENCLOSURE~~

~~Derived from : G-3~~
~~Declassify on: X25-1~~

General Brent Scowcroft (USAF Retired)

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience.

Sincerely,

Julie F. Thomas
Deputy General Counsel

1 - The Honorable Alberto Gonzales
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James Baker
Counsel for Intelligence Policy, OIPR
U.S. Department of Justice

NEEDS
ORIGINAL REPORT
EC AND
OPINION FROM
OGC

U.S. Department of Justice

Federal Bureau of Investigation

~~SECRET~~

Washington, D. C. 20535-0001

February 11, 2004

BY COURIER

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, Northwest
Washington, D.C.

Dear General Scowcroft:

Enclosed for your information is a self-explanatory memorandum, entitled "Intelligence Oversight Board (IOB) Matter, Pittsburgh Division, IOB Matter 2002-57" (U)

This memorandum sets forth details of investigative activity which the FBI has determined was conducted contrary to the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. This matter has also been referred to our Office of Professional Responsibility for a determination of whether any administrative action is warranted. (U)

Enclosure

~~UNCLASSIFIED WHEN DETACHED FROM CLASSIFIED ENCLOSURE~~

1 - Mr. Szady
1 - OPR (IOB 2002-57)
1 - 278-HQ- 1400430-4
1 - [redacted]

~~Derived from : G-3~~
~~Declassify on: X 25-1~~

b6
b7C

~~SECRET~~

FBI - OPR
4 2 2004

Asst. Dir.
Admin. Ser
Crim. Inv
CJIS
Finance
Info. Res.
Lab.
National Sec
OPR
Off. of Public & Cong. Affs.
Training
Off. of EEOA
Director's Office

MAIL ROOM

FBI/DOJ

~~SECRET~~

General Brent Scowcroft (USAF Retired)

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience. (U)

Sincerely,

Patrick W. Kelley
Deputy General Counsel

1 - Honorable John D. Ashcroft
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. H. Marshall Jarrett
Counsel, Office of Professional Responsibility
U.S. Department of Justice
Room 4303

1 - Mr. James Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

APPROVED:
Director
Deputy Director
Gen. Counsel
Info. Res.
Personnel
Off. of Public &
Cong. Affs.

LDK
CTLU I

~~SECRET~~

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
PITTSBURGH DIVISION
IOB MATTER 2002-57 (U)

Inquiry has determined that in conducting a preliminary inquiry (PI) of a United States person, the Federal Bureau of Investigation (FBI) failed to comply with the requirements for the continuation of a PI as prescribed in Section III.B.6 of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). In this regard, the Pittsburgh Division opened a PI on a sensitive asset on 03/21/02 to determine his/her suitability as an asset for foreign counterintelligence matters. The initial 120-day PI was not extended but contact between the asset and the Special Agent continued. The Agent discovered the error on 09/26/02. In mitigation of the errors, Pittsburgh advised that the only investigative actions taken following the expiration of the initial 120-day authorization were a series of electronic mail (e-mail) communications. One e-mail concerned the scheduling of a security briefing, while the remaining e-mails were social in nature. Because the subject was (and remains) a "United States person" as that term is used in Section 101(i) of the Foreign Intelligence Surveillance Act of 1978, continuation of the investigation required that Pittsburgh comply with the requirements of Executive Order 12863 and the FCIG. In this matter, while the PI overrun appears to have been inadvertent, it was not de minimis in time. The PI was never properly extended, and investigative activity occurred for approximately two months after the PI had expired. Therefore, this report is being made to the Intelligence Oversight Board. ~~(S)~~ (U)

~~Derived from : G-3~~
~~Declassify on: X 25-1~~

APPROVED:
Director
Deputy Director
Crim. Inv. | Inspection | Training
CJIS | Laboratory | Off. of EEO
Finance | National Sec. | Affairs
Gen. Counsel | [illegible] | Off. of Public &
Info. Res. | Personnel | Cong. Affs.

~~SECRET~~

LDK
CTLU I

Access Denied -

Precedence: ROUTINE Date: 08/26/2004

To: Director's Office Attn: OPR
Counterintelligence Attn: AD
Washington Field Attn: SAC/CI
CDC

From: General Counsel
Counterintelligence Law Unit/Room 7975
Contact: [redacted]

Approved By: Curran John F [redacted]

Drafted By: [redacted]

b6
b7C

Case ID #: (U) 278-HQ-C1229736-VIO (Pending)
~~(S)~~ (U) 65J-WF-A1419323 (Pending)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD MATTER
IOB 2004-58

Synopsis: (S) The Office of the General Counsel (OGC) considers that this matter must be reported to the Intelligence Oversight Board (IOB) and to the Office of Professional Responsibility (OPR). Our analysis follows.

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

DATE: 08-12-2005
CLASSIFIED BY 65179DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-12-2030

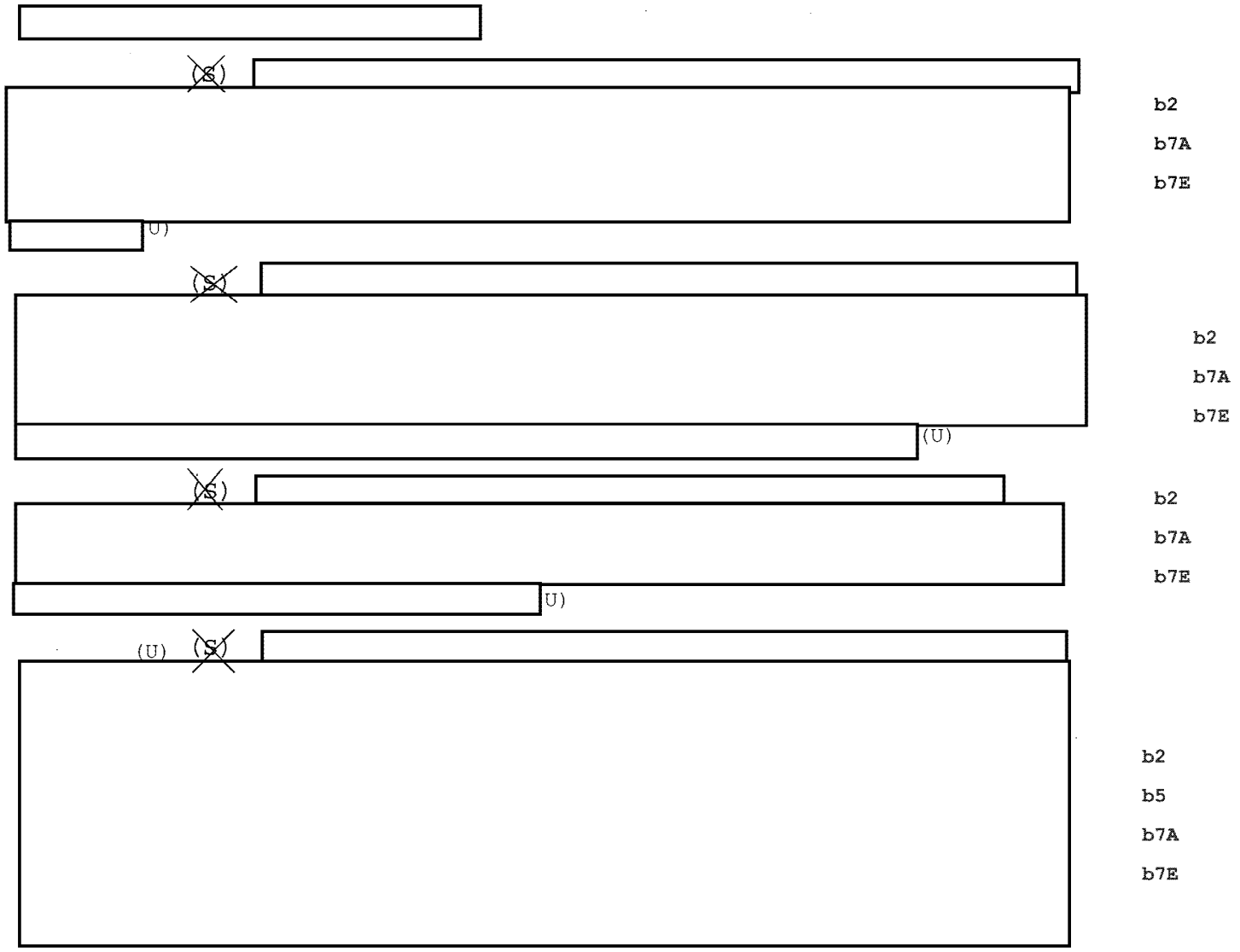
Details: ~~(S)~~ [redacted]

[redacted] (S)

b1
b2
b7A
b7E

~~[redacted]~~ [redacted] (S)

b2
b7A
b7E



b2
b7A
b7E
b2
b7A
b7E
b2
b7A
b7E
b2
b5
b7A
b7E

(U) Even though the violation was technical, it is nonetheless reportable to the IOB under the provisions of Section 2.4 of E.O. 12863. Consequently, OGC will prepare a cover letter and a memorandum to report this matter to the IOB. The correspondence will advise the IOB that the matter will be referred to the FBI's OPR.

LEAD(s):

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 2: (Info)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) Please read and clear.

Set Lead 3: (Action)

WASHINGTON FIELD

AT WASHINGTON, DC

(U) For action deemed appropriate.

BY COURIER

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure entitled, "Intelligence Oversight Board (IOB) Matter, IOB 2004-58." (U)

The enclosure sets forth details of investigative activity which the FBI has determined was conducted contrary to the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

Enclosure

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~UNCLASSIFIED WHEN~~
~~DETACHED FROM~~
~~CLASSIFIED ENCLOSURE~~

DATE: 08-15-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-15-2030

~~Classified by: 39431, FBI/OGC~~
~~Reason: 1.5(c)~~
~~Declassify on: X25-1~~

1 - Mr. Curran
1 - [redacted]
1 - IOB Library
1 - 278-HQ-C1229736-VIO

b6
b7C

General Brent Scowcroft (USAF Retired)

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience.

Sincerely,

John F. Curran
Deputy General Counsel

1 - The Honorable John D. Ashcroft
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
IOB 2004-58 (U)

~~(S)~~ Investigation of this IOB matter has determined that

[redacted] b2 b7A b7E

~~(S)~~ [redacted] (S)

[redacted] (S) b1 b2 b7A b7E

(U) Nevertheless, a technical violation of E.O. 12333 occurred. This matter has been referred to the FBI's Office of Professional Responsibility for any action that is deemed appropriate.

~~Derived from: G-3~~
~~Declassify on: X25-1~~

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 16
Page 31 ~ Duplicate Undated Letter re: IOB Matter 2004-77, pg. 1
Page 32 ~ Duplicate Undated Letter re: IOB Matter 2004-77, pg. 2
Page 33 ~ Duplicate Undated Summary re: IOB Matter 2004-77
Page 40 ~ Duplicate Undated Letter re: IOB Matter 2004-21, pg. 1
Page 41 ~ Duplicate Undated Letter re: IOB Matter 2004-21, pg. 2
Page 106 ~ Duplicate Undated Summary re: IOB Matter 2004-21
Page 112 ~ Duplicate EC dated 10/22/04 re: IOB Matter 2003-56
pg. 1
Page 113 ~ Duplicate EC dated 10/22/04 re: IOB Matter 2003-56
pg. 2
Page 114 ~ Duplicate EC dated 10/22/04 re: IOB Matter 2003-56
pg. 3
Page 115 ~ Duplicate EC dated 10/22/04 re: IOB Matter 2003-56
pg. 4
Page 116 ~ Duplicate EC dated 10/21/04 re: IOB Matter 2004-77
pg. 1
Page 117 ~ Duplicate EC dated 10/21/04 re: IOB Matter 2004-77
pg. 2
Page 118 ~ Duplicate EC dated 10/21/04 re: IOB Matter 2004-77
pg. 3
Page 119 ~ Duplicate Undated Letter re: IOB Matter 2004-77, pg. 1
Page 120 ~ Duplicate Undated Letter re: IOB Matter 2004-77, pg. 2
Page 121 ~ Duplicate Undated Summary re: IOB Matter 2004-77

Precedence: ROUTINE Date: 08/27/2004

To: General Counsel Attn: NSLB
Inspection

From: [redacted] b2 b7E
CT-4
Contact: SA [redacted] b2 b6 b7C

Approved By: [redacted] b6 b7C

Drafted By: [redacted] bsc

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE
DATE: 12-03-2005
CLASSIFIED BY 65179DMH/BAW 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-03-2030

Case ID #: ~~(S)~~ (U) 278-HQ-C1229736-VIO

Title: (U) PRESIDENT'S INTELLIGENCE OVERSIGHT BOARD

Synopsis: (S) [redacted] b1

~~(S)~~ (U) ~~Derived From : G-3~~ b1
~~Declassify On: X1~~

Details: (S) [redacted] b1

(S) [redacted] b1 b6 b2 b7A b7E b7C

(S) [redacted] b7A b2 b7E

(S) [redacted] b1 b2 b7A b6 b7C b7E

Case ID : 278-HQ-C1229736-VIO Serial : 572

11/3/9/05

(S)

(S)

b1
b2
b7E
b7A
b6
b7C

LEAD(s):

Set Lead 1: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) For the information of OGC and for any further action at the discretion of OGC.

Set Lead 2: (Info)

INSPECTION

AT WASHINGTON, DC

(U) For the information of Inspection and for any further action at the discretion of Inspection.

10B5733. WPD

(Rev. 01-31-2003)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/08/2005

To: [redacted] b2 b7E **Attn:** SAC
CDC

Counterterrorism **Attn:** ITOS I / CONUS IV
SSA [redacted] b6 b7C

Inspection **Attn:** IIS
SC Toni Fogle

From: General Counsel
NSLB/CTLU I/Room 7975
Contact: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Approved By: Thomas Julie F [redacted] b6

Drafted By: [redacted] rm b7C

b2 b7E **Case ID #:** (S) [redacted]278-HQ-C1229736-VIO (Pending) [redacted] (Pending) b6 b7C

b7A **Title:** (U) INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER 2004-79 [redacted]

To me - but still an "OPR" lead (?) Plea handle & corr lead as RMS. MA

Synopsis: (S) (U) It is the opinion of the Office of General Counsel (OGC) that the above referenced matter must be reported to the Intelligence Oversight Board (IOB) and to the FBI's Office of Professional Responsibility (OPR). Our analysis follows.

(S) (U) ~~Derived From : G-3~~ [redacted] ~~Declassify On: X1~~

DATE: 09-12-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-12-2030

Reference: (S) (U) 278-HQ-C1229736-VIO Serial 572

Details: (S) [redacted] b1 b2 b7E b6 b7C b7A

~~SECRET~~

OIG/DOJ Review: Vamy DATE: 8/20/05
FBI INVEST.: M OIG/DOJ INVEST.: _____
OPR UC INITIALS: _____

To: [redacted] From: General Counsel
Re: (S) (U) 278-HQ-C1229736-VIO, 02/08/2005

b1
b2
b7E
b7A

[redacted] (S)

(S) [redacted]

(U) Title 18, United States Code, Section 2511, prohibits the interception of electronic communications [redacted] except as provided by law. The act includes an exception for electronic surveillance that is conducted in accordance with the terms of the Foreign Intelligence Surveillance Act. 18 U.S.C. 2511(2)(e). In this case, however,

b2
b7E

b1
b2
b7E
b7A

[redacted] (S)

b1
b2
b7E

(U)[1] (S) A "United States person" is defined in section II.W of the Guidelines as "an individual who is . . . [a] United States citizen . . . or . . . a permanent resident alien . . . ." This regulatory definition is based on the definition of a "United States person" as that term is used section 101(i) of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801 et seq. The latter states, in pertinent part, that a "'United States person' means a citizen of the United States [or] an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . ."

To: [redacted] From: General Counsel b2
Re: (S) 278-HQ-C1229736-VIO, 02/08/2005 b7E
(U)

Thus, the interception of these communications was not authorized.

(U) Section 2.4 of Executive Order 12863 of September 13, 1993, requires General Counsel of the intelligence community to report intelligence activities that they have reason to believe may be unlawful or contrary to executive orders or presidential directives to the Intelligence Oversight Board. The circumstances of this case show that [redacted] (S) Although a narrow reading of E.O. 12863 might not require the FBI to report this mistake to the Intelligence Oversight Board, the Office of the General Counsel has traditionally done so in these kinds of cases. OGC has therefore prepared an appropriate communication to the Intelligence Oversight Board and to the Inspection Division, Internal Investigations Section. b1 b2 b7E

To: [redacted] From: General Counsel
Re: (S) [redacted] 278-HQ-C1229736-VIO, 02/08/2005

b2
b7E

LEAD(s):

Set Lead 1: (Discretionary)

[redacted]

AT [redacted]

(U) For appropriate action.

Set Lead 2: (Discretionary)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For appropriate action.

Set Lead 3: (Info)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) For information only.

♦♦

~~SECRET~~

BY COURIER

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure entitled, "Intelligence Oversight Board (IOB) Matter, IOB 2004-79." (U)

The enclosure sets forth details of investigative activity which the FBI has determined may have been contrary to the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

1 - Ms. Thomas
1 - [redacted]
1 - [redacted]

1 - IOB Library
1 - 278-HQ-C1229736-VIO

b6
b7C

~~Derived from: G-3~~
~~Declassify on: X25-1~~

~~SECRET~~

~~SECRET~~

General Brent Scowcroft (USAF Retired)

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience.

Sincerely,

Julie Thomas
Deputy General Counsel

Enclosure

1 - The Honorable Alberto R. Gonzalez
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

~~SECRET~~

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
IOB 2004-79 (U)

~~(S)~~ The FBI received authorization from the Foreign Intelligence

(C) (S)

b1
b2
b6
b7C
b7E
b7A

(S)

b1
b2
b7E
b7A

(S)

b1
b7A
b2
b7E

(S)

b1
b7A
b2
b7E

Internal Investigations
Section for any action that is deemed appropriate. (U)

~~SECRET~~

~~Derived from: G-3~~
~~Declassify on: X-1~~

#1647

~~SECRET~~
---- Working Copy ----

Precedence: ROUTINE

Date: 06/22/2003

To: Counterintelligence

Attn: SSA [redacted]
CD-1D
IMU
NSLU

Inspection
General Counsel

DATE: 12-03-2005
CLASSIFIED BY 65179 DMH/BAW
REASON: 1.4 (C)
DECLASSIFY ON: 12-03-2030

From: [redacted]
Squad 6
Contact: SA [redacted]

Approved By: Whitehead Carl

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2
b7E
b6
b7C

Drafted By: [redacted]

Case ID #: (S) [redacted] (Pending)
(S) 278-HQ-C1229735 (Pending)
(S) 278-HQ-C1229736-VIO (Pending)

b1
b2
b7E

Title: ~~(S)~~ (U) INTELLIGENCE OVERSIGHT BOARD;
SSA [redacted]
SA [redacted]

b7A
b1
b7A

(S) [redacted]

b2
b7E

Synopsis: (S) [redacted]

b1
b2
b7E
b7A

~~(S)~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

(S) [redacted]

Package Copy: (S) [redacted]

Case ID : 278-HQ-C1229736 1797 (S)
278-HQ-C1229736-VIO 107
278 [redacted] C63856-VIO 3

b1
b2
b7E
b7A

~~SECRET~~

b2
b7E

09/09/05

(S)

Details: (S)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

b1
b2
b7E
b6
b7C
b7A

(S)

(S)

(S)

(S)

(S)

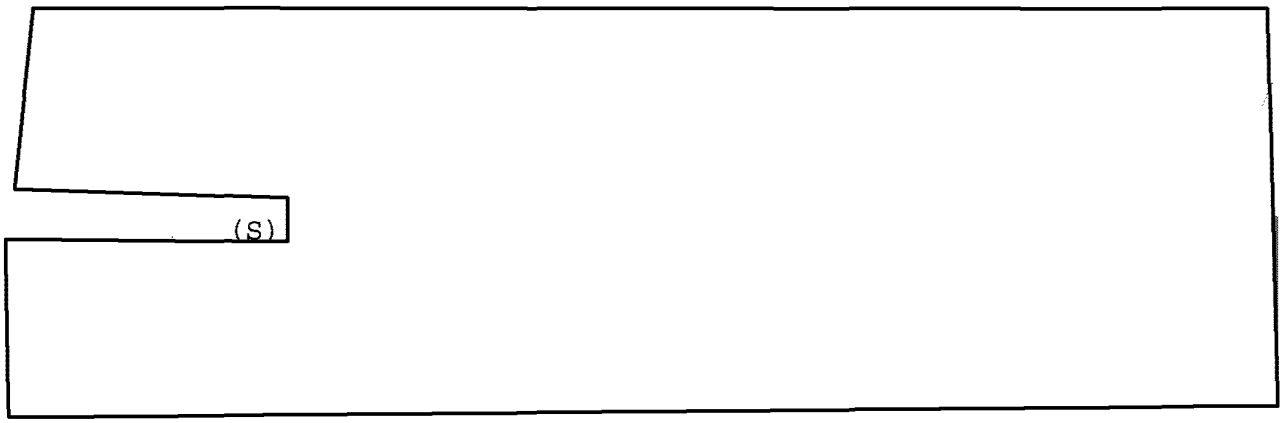
(S)

(S)

(S)

(S)

b1
b2
b7E
b6
b7C
b7A



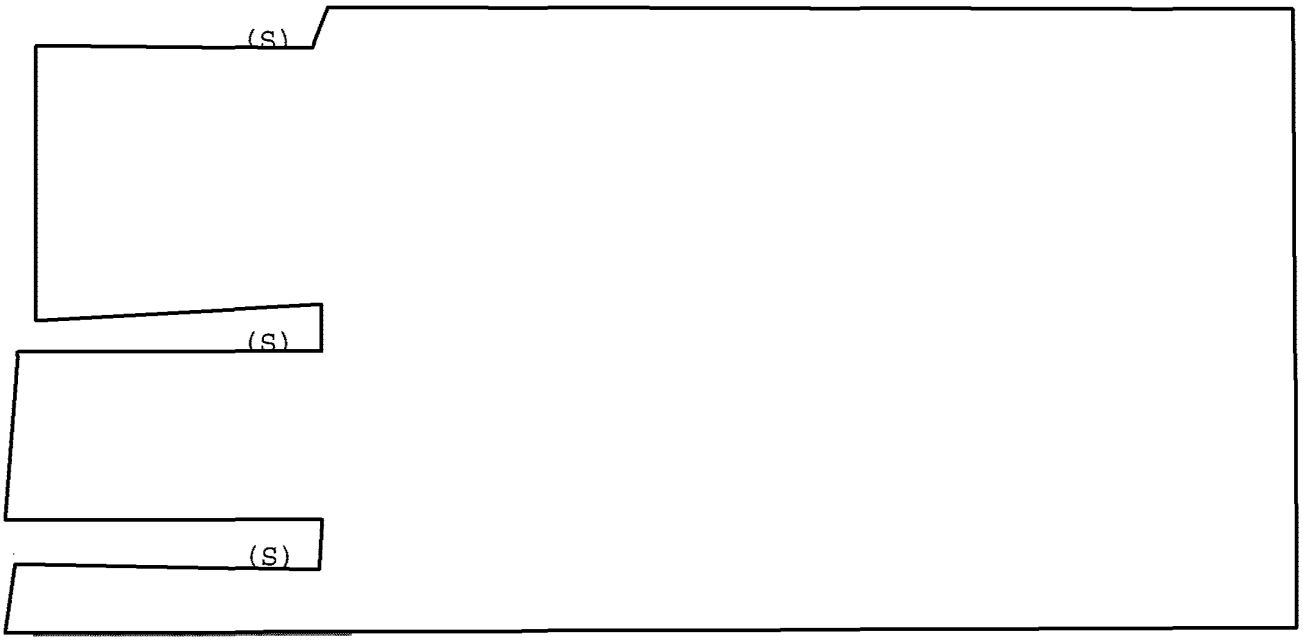
b1
b2
b7E
b6
b7C
b7A

LEAD(s):

Set Lead 1: (Action)

COUNTERINTELLIGENCE

AT WASHINGTON, DC



b1
b2
b7E
b6
b7C
b7A

January 4, 2005

General Brent Scowcroft (USAF Retired)
Chairman Intelligence Oversight Board
New Executive Office Building
Washington, D.C.

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure entitled "Intelligence Oversight Board (IOB), Matter 2004-96." (U)

The enclosure sets forth details of investigative activity which the FBI has determined was conducted contrary to the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

Enclosure

1 - Mr. Szady
1 - SAC [redacted]
1 - Ms. Thomas
1 - [redacted]
1 - OPR
1 - 278-HQ-C1229736-VIO

b2
b7E
b6
b7C

~~UNCLASSIFIED WHEN~~
~~DETACHED FROM~~
~~CLASSIFIED ENCLOSURE~~

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience. (U)

Very truly yours,

Julie F. Thomas
Deputy General Counsel

1 - The Honorable John D. Ashcroft
Attorney General
U.S. Department of Justice
Room 5111

2 - Mr. James A. Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

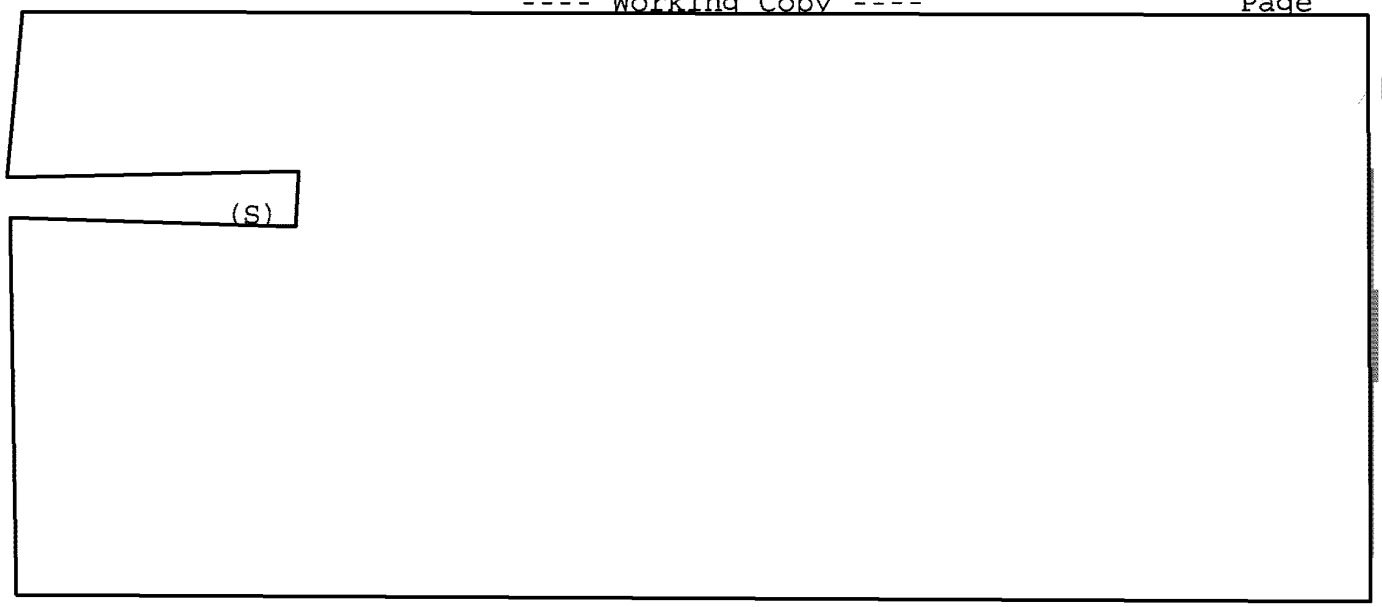
b1
b2
b7E
b6
b7C
b7A

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER [redacted] DIVISION
IOB MATTER 2004-96 (U)

(S)

(S)

(S)



b1
b2
b7E
b6
b7C
b7A

Precedence: PRIORITY Date: 07/16/2004

To: General Counsel Attn: National Security Law Branch
Counterintelligence Attn: CD-3B, Room 4094
SSA [redacted]

From: [redacted]
Squad 16B, [redacted] RA
Contact: SA [redacted]

Approved By: Mershon Mark J
[redacted]

Drafted By: [redacted]

Case ID #: ~~(S)~~ 278-HO-C1229736-VIC (U) (Pending)
(S) [redacted]

Title: ~~(S)~~ (U) SSRA [redacted]
SA [redacted]
[redacted] Division
IOB

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

b1
b2
b7E
b6
b7C

DATE: 12-03-2005
CLASSIFIED BY 65179DMH/BAW 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-03-2030

Synopsis: (U) ~~(S)~~ Notification to the Office of General Counsel of potential Intelligence Oversight Board (IOB) violation(s).

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

~~Enclosure(s):~~ (S) [redacted]

b1
b2
b7E
b7A

Detail: (U) ~~(S)~~ As directed per EC dated 03/08/2004 from the National Security Law Branch, this communication is provided as notification to the Office of General Counsel of potential IOB violation(s).

b1
b2
b7E
b7A

(S) [redacted]
(S)

Case ID : 278-HO-C1229736-VIO [redacted] Serial : 556

278- -C136372 (S) (S) 39

~~SECRET~~

b1
b2
b7E

11/09/05

b1
b7A

(S)

(S)

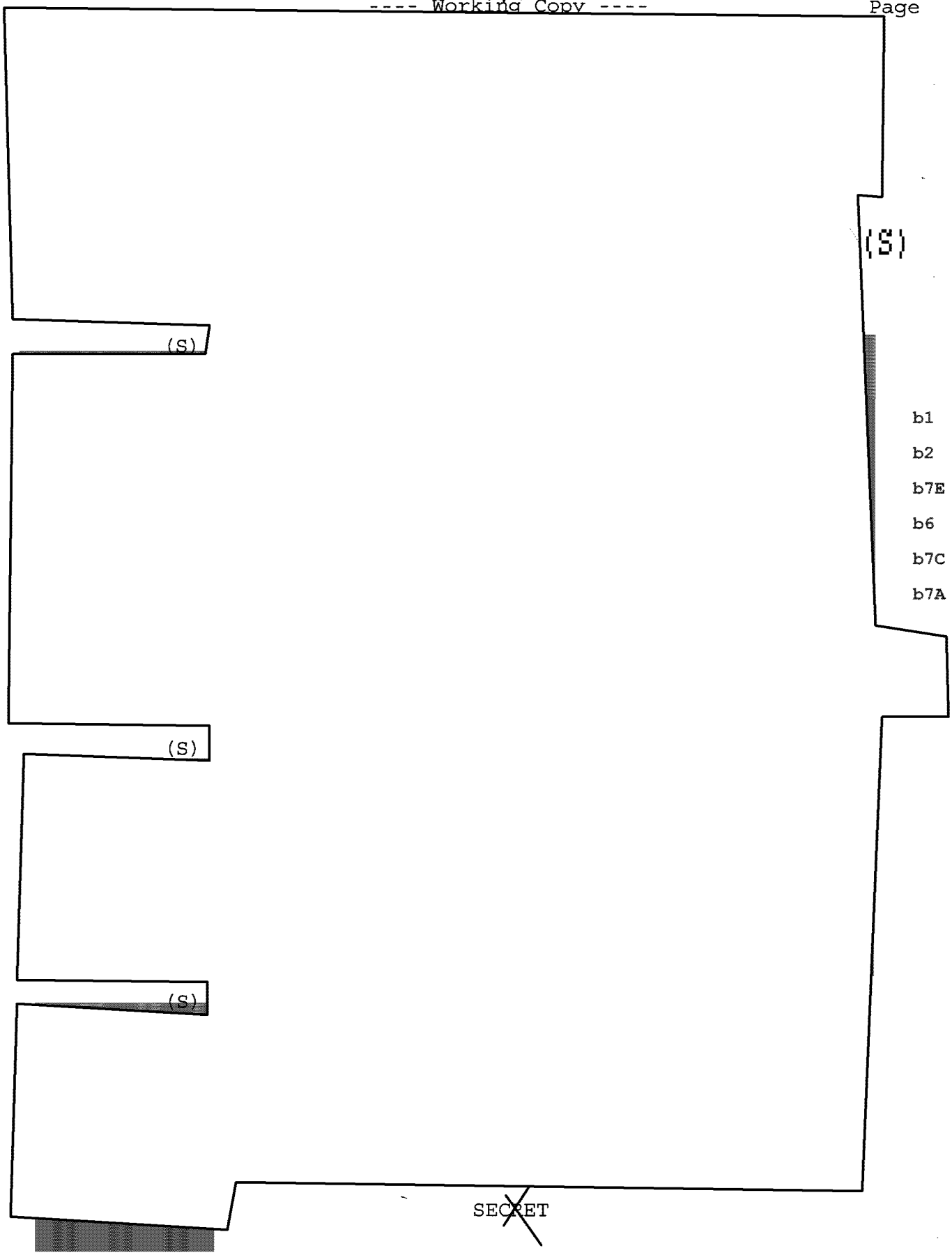
(S)

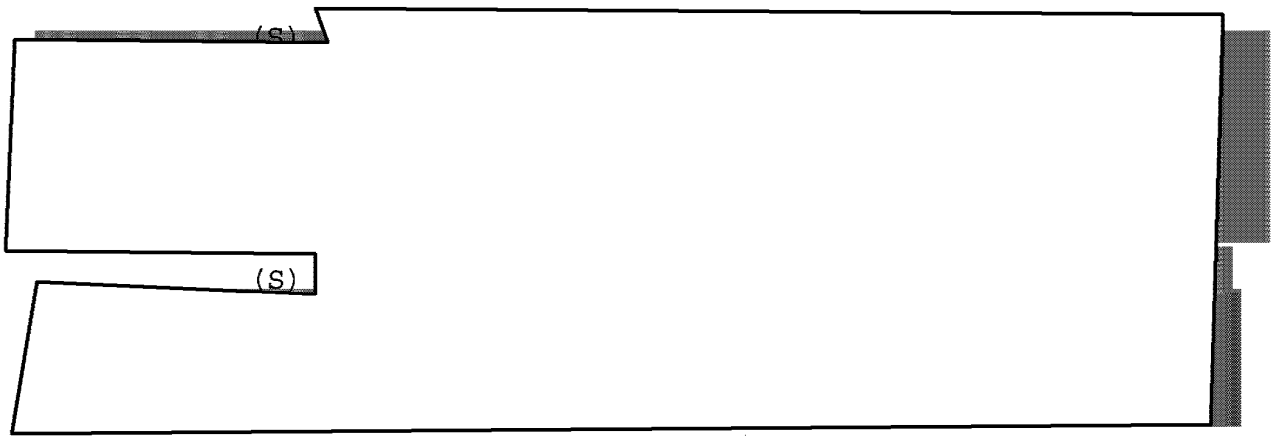
(S)

(S)

(S)

b1
b2
b7E
b6
b7C
b7A


(S)
(S)
(S)
(S)
b1
b2
b7E
b6
b7C
b7A



b1
b2
b7E
b7A

LEAD(s):

Set Lead 1: (Discretionary)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) (S) As directed per EC dated 03/08/2004 from the National Security Law Branch, this communication is provided as notification to the Office of General Counsel of potential IOB violation(s).

Set Lead 2: (Info)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) (S) Read and clear.

Precedence: ROUTINE Date: 11/24/2004

To: [redacted] Division Attn: ASAC FCI/Administrative CDC
Counterintelligence Attn: CD-3B, Room 4094
SSA [redacted]
Director's Office Attn: Office of Professional Responsibility

From: General Counsel
National Security Law Branch/CILU/Room 79875
Contact: [redacted]

Approved By: Thomas Julie F [redacted]

Drafted By: [redacted]

Case ID #: (S) 278-HQ-C1229736-VIO (U) (Pending)
(S) [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Title: (S) (U) Intelligence Oversight Board (IOB) Matter 2004-75

Synopsis: (S) (U) It is the opinion of the Office of General Counsel (OGC) that the above referenced matter must be reported to the IOB and to the FBI's Office of Professional Responsibility (OPR). OGC will prepare and deliver the required correspondence to the IOB. Our analysis follows.

DATE: 12-03-2005
CLASSIFIED BY 65179DMH/BAW/05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-03-2030

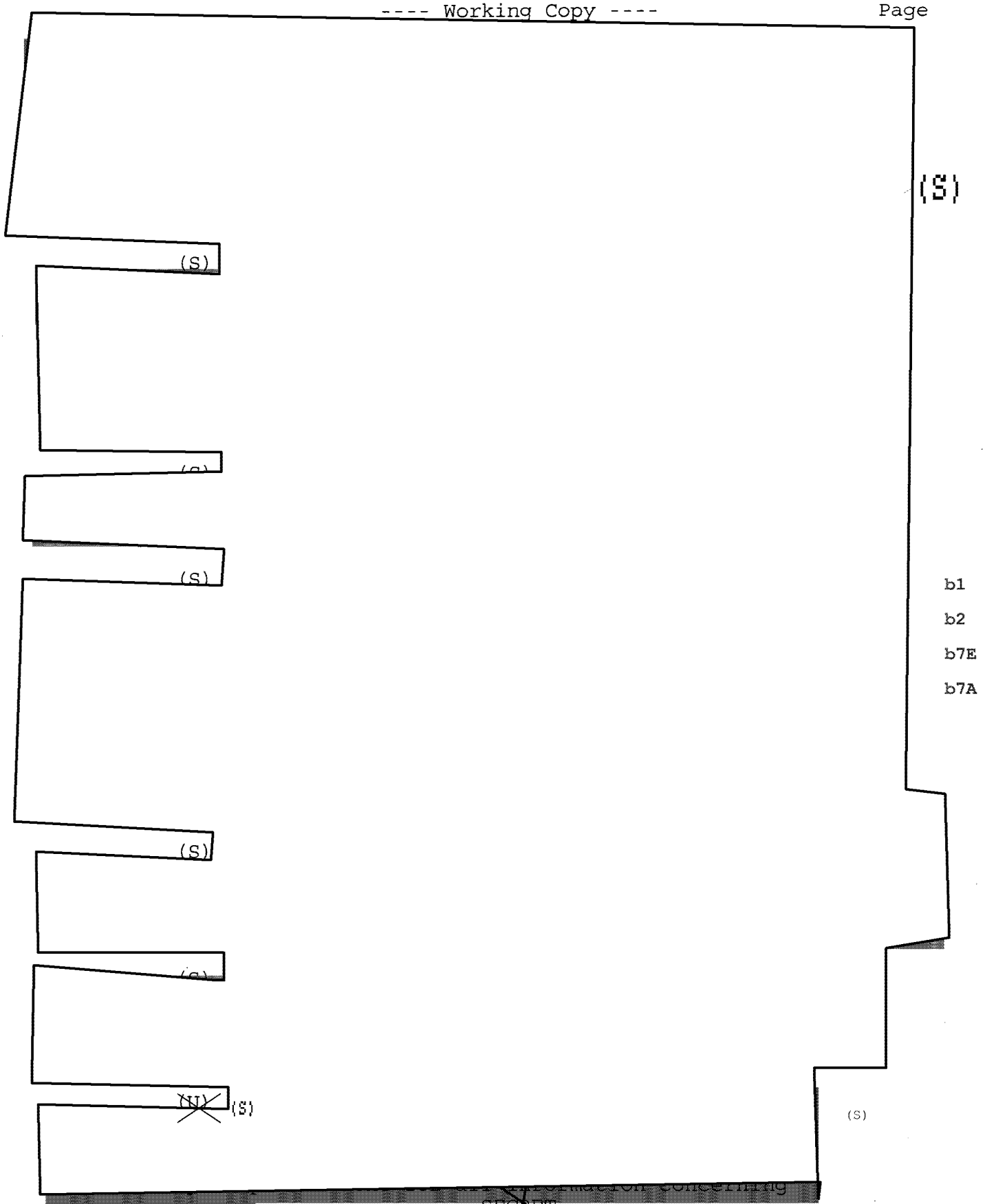
(S) (U) ~~Derived From : G-3~~
~~Declassify On: 08/03/2029~~

Reference: (S) (U) 278-HQ-C1229736-VIO Serial 556

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in Corel WordPerfect.

Details: (S) [redacted]

b1
b2
b7E
b6
b7C
b7A
b1
b7A



b1
b2
b7E
b7A

(S) b1 b2 b7A

FOOTNOTES

ï1´: (U) See EC from the Division to the General Counsel, dated July 16, 2004, Case ID# 278-HQ-C1229736-VIO Serial 556, titled "SSRA SA Division, IOB" hereinafter cited as EC." b2 b7E b6 b7C

ï2´: (U) EC (S)

ï4´: (U) EC. b1 b2 b7A

ï5´: (U) Id.

ï6´: (U) Id.

ï7´: (U) Id. This notification was made via FBI e-mail.

ï8´: (U) EC. The FBI technical collection personnel so informed by reply e-mail.

ï9´: (U) EC. b1 b2 b7A

ï10´: (U) Id.

ï11´: (U) Id. (S)

ï12´: (U) (S)

ï13´: (U) EC. AGC gave the unopened envelope containing this information to SSA CD-3B who then b6 b7C

submitted the unopened envelope to the [redacted]

ï14´: (U) [redacted] EC.

ï15´: (U) Id.

LEAD(s):

Set Lead 1: (Info)

[redacted]

AT [redacted]

(U) [redacted] is requested to identify and forward all material acquired [redacted] to CD-3B.

Set Lead 2: (Action)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) CD-3B is requested to ensure that all material provided by [redacted] be submitted [redacted]

Set Lead 3: (Discretionary)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For review and action deemed appropriate.

CC: Ms. Thomas

[redacted]

NSLB IOB Library

b6
b7C
b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

BY COURIER

DATE: 12-03-2005
CLASSIFIED BY 65179DMH/BAW 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-03-2030

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
New Executive Office Building
Washington, D.C.

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure entitled Intelligence Oversight Board (IOB) Matter, [redacted] Division, IOB Matter 2004-75." (U) b2 b7E

The enclosure sets forth details of investigative activity which the FBI has determined was conducted contrary to the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

Enclosure

b6
1 - Mr. Szady
1 - Mr. Curran b7C
1 - [redacted]
1 - 278-HQ-C1229736-VIO-

~~UNCLASSIFIED WHEN DETACHED FROM CLASSIFIED ENCLOSURE~~

OIG/DOJ Review: Vong DATE: 5/20/05
FBI INVEST.: (W) OIG/DOJ INVEST.:
OPR UC INITIALS:

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience. (U)

Sincerely,

John F. Curran
Deputy General Counsel

1 - The Honorable John D. Ashcroft
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James A. Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER [redacted] b2 b7E

IOB MATTER 2004-75 (U)

(S) [redacted] b1 b2 b7E

[redacted] (S)

b1
b2
b7E

(S) [redacted]

b1
b2
b7E

(S) [redacted]

b1
b2
b7E

(S) [redacted]

b1
b2
b7E

(S) [redacted]

b1
b2
b7E

(U) This matter has been reported to the FBI's Office of Professional Responsibility for appropriate action.

~~Derived from : G-3~~
~~Declassify on: X1~~

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 4
Page 28 ~ Duplicate
Page 29 ~ Duplicate
Page 30 ~ Duplicate
Page 31 ~ Duplicate

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

BY COURIER

DATE: 10-13-2005
CLASSIFIED BY 65179DMH/lr2 Ca#05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 10-13-2030

General Brent Scowcroft (USAF Retired)
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure entitled, "Intelligence Oversight Board (IOB) Matter, IOB 2004-81." (U)

The enclosure sets forth details of investigative activity which the FBI has determined may have been contrary to the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

UNCLASSIFIED WHEN
DETACHED FROM
CLASSIFIED ENCLOSURE

1 - Mr. Curran
1 - [redacted]
1 - [redacted]
1 - IOB Library
1 - 278-HQ-C1229736-VIO

b6
b7C

~~Derived from: G-3~~
~~Declassify on: X25-1~~

~~SECRET~~
~~SECRET~~
-2-

General Brent Scowcroft (USAF Retired)

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience.

Sincerely,

Julie Thomas
Deputy General Counsel

Enclosure

1 - The Honorable John D. Ashcroft
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

UNCLASSIFIED WHEN
DETACHED FROM
CLASSIFIED ENCLOSURE

~~Derived from: G-3~~
~~Declassify on: X25-1~~

~~SECRET~~

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
IOB 2004-81 (U)

~~(S)~~ ~~The~~ FBI received authorization from the Foreign Intelligence

Surveillance Court (FISC) on August 5, 2004, to use a pen register and trap and trace device to collect [redacted] electronic communications originating from or received at [redacted] that were used by a U.S. person who is the subject of an ongoing counterintelligence investigation. [redacted]

The order specified that the following information was to be collected: [redacted] the source/destination, dates and times of such communications and the "To:," "From:," "cc:," and "Received:" headers for those communications but not the content of such communications as defined by 18 U.S.C. 2510 (8)." (Emphasis added [redacted]

(S) On August 30, 2004, [redacted] provided the initial response to the order in the form of two original compact disks (CDs) marked [redacted] August 30 2004 12:58 CDT. The Case Agent reviewed the material on August 31, 2004. On inspecting the CDs, the Case Agent realized that [redacted] The FBI promptly informed [redacted] of the error and asked that henceforth only the information specified in the order be provided. The original CDs were sent by the Office of the General Counsel to the Office of Intelligence Policy and Review for appropriate disposition. No copies of the contents of the [redacted] were retained by the FBI.

(S) The interception of electronic communications in this case resulted from an error on the part of the internet service provider; nevertheless, the interception was unauthorized and thus contrary to Title 18, United States Code, Section 2511. The matter is therefore reportable to the Intelligence Oversight Board under the terms of Executive Order 12863. In addition, it has been referred to the FBI's Office of Professional Responsibility for any action that is deemed appropriate.

~~SECRET~~

Derived from: G-3
Declassify on: X-1

Precedence: ROUTINE
Date: 12/10/2003

To: Counterterrorism
Attn: ITOS 1/CONUS 1/Team 2
SSA [redacted]

General Counsel
Attn: NSLB/CTLU II
[redacted] b6 b7C

[redacted] b2 b7E
Attn: [redacted]
SSA [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

From: [redacted]
CT-1
Contact: SA [redacted]

Approved By: Kaiser Kenneth W
[redacted] b2 b6 b7C

DATE: 10-13-2005
CLASSIFIED BY 65179DMH/lr2 Ca# 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 10-13-2030

Drafted By: [redacted] :gth

Case ID #: (U) 278-HQ-C1229736-VIO (Pending)

Title: (U) PRESIDENTIAL INTELLIGENCE OVERSIGHT BOARD (IOB)

Synopsis: ~~(U)~~ [redacted] (S)

[redacted] b1 b2 b7E

~~(S)~~ Derived From : ~~G-3~~
Declassify On: ~~X1~~

Reference: (U) 66F-HQ-A1247863 Serial 130

Details: ~~(S)~~ U Consistent with the guidelines set forth in the referenced communication, [redacted] Division reports that [redacted] inadvertently recorded pen/toll information from a subject's home telephone line after the subject changed numbers. The pen register/trap and trace device [redacted] was disabled [redacted] (S) (S)

b1 b2 b7E

~~(S)~~ U The pen/toll information was recorded through a United States Foreign Intelligence Surveillance Court (USFISC) authorized installation of a pen register/trap and trace device [redacted] (S)

~~(S)~~ U Controlling legal authority for the relevant investigation is as follows:

---

b1
b2
b6
b7C
b7E

(S)

(USPER)
IT-UBL/AL-QAEDA
315N-[redacted]-89623

(S)

(S)

b1
b2
b7E
b6
b7C

(U)

serviced by

(S)

(S)

(S)

(S)

(S)

(S)

b1
b2
b7E
b6
b7C

(S)

(S)

LEAD(s):

Set Lead 1: (Info)

COUNTERTERRORISM

AT WASHINGTON, D.C.

(U) Read and clear.

Set Lead 2: (Action)

GENERAL COUNSEL

AT NSLB

1. (U) NSLB is requested to coordinate with ITOS 1/CONUS 1/Team 2 and DOJ/OIPR to ensure required reporting mandates are met.

2 (U) [redacted] b2 b7E

Precedence: ROUTINE b2 Date: 03/18/2005

b7E

To: [redacted] Attn: SAC
CDC

Counterterrorism Attn: AD

Inspection Attn: Internal Investigation
Section (IIS)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

From: General Counsel
National Security Law Branch/LX Crossing, Room 5S200
Contact: [redacted] b2 b6

Approved By: Thomas Julie F [redacted]

DATE: 10-13-2005
CLASSIFIED BY 65179DMH/lr2 Ca#-05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 10-13-2030

b7C

Drafted By: [redacted]

Case ID #: ~~(S)~~ 278-HQ-C1229736-VIO (Pending)

Title: ~~(S)~~ SA [redacted]
SA
INTELLIGENCE OVERSIGHT BOARD
(IOB) MATTER 2004-71

b6
b7C

Synopsis: ~~(S)~~ It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB)and to the Office of Professional Responsibility (OPR), FBIHQ. OGC will prepare and deliver the necessary correspondence to the IOB. Our analysis follows.

~~(S)~~ ~~Derived from : G-3~~
~~Declassify On: X25-1~~

Tickle & cover in ACS. 5/12

Reference: (S) 278-HQ-C1229736-VIO Serial 546
278-HQ-C1229736-VIO Serial 298

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect 6.1.

(S)

b1
b2
b7E
b6
b7C

(S)

[redacted] (S) b1 b2 b7E

Also on that same day, OGC, as well as International Terrorism Operations Section 1 (ITOS 1), were notified of the error, both orally and by EC dated 12/10/2003.

[redacted] (S) b1 b2 b7E

(U) Measures have been taken by [redacted] to prevent a recurrence of this error. The TTA who made the above-described error has been counseled to not delete any email messages without reading it. Further, the case agent and all technical personnel have been instructed to communicate by personal contact all pertinent information regarding technical coverage to the appropriate TTA or technical supervisor. It has been made clear that it is the responsibility of each agent/investigator to verify by contact with the technical squad and a query in ACS that [redacted] b2 b7E

(U) Section 2-56 of the National Foreign Intelligence Program Manual (NFIPM) requires OGC to determine whether the facts related above are required to be reported to the IOB.

Section 2.4 of Executive Order (EO) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive."

(S) Appl
concludes tha
(S)

b1
b2
b7E

The case agent intended that this would happen. However, it did not. Consequently, in accordance with E.O. 12863 and Section 2-56 of the NFIPM, the inadvertent error must be reported to the IOB, which this Office will do.

LEAD (s):

Set Lead 1: (INFO)

b2
b7E

[redacted]

AT [redacted]

(U) Read and clear.

Set Lead 2: (Action)

INSPECTION

AT INTERNAL INVESTIGATION SECTION, DC

(U) For action deemed appropriate.

Set Lead 3: (Action)

COUNTERTERRORISM

AT WASHINGTON, D.C.

(U) For action deemed appropriate

1 - Ms. Thomas
1 - [redacted]
1 - [redacted]
1 - IOB File

b6
b7C

FOOTNOTES

ï1´: (S) (U) United States person is defined in Section 101(i) of the Foreign Intelligence Surveillance Act (FISA)(codified at 50 U.S.C. 1801 et seq.) as a citizen of the United States ïor´ an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . . See also Section I.C of The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG).

ï2´: (S) The case agent does not remember the date in December on which the

[redacted] (S)

b1
b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

BY COURIER

DATE: ~~10-13-2005~~ (C)
CLASSIFIED BY 65179DMH/lr2 Ca#-05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 10-13-2030

Mr. James Langdon
Chairman
Intelligence Oversight Board
New Executive Office Building
Washington, D.C.

Dear Mr. Langdon:

Enclosed for your information is a self-explanatory memorandum, entitled "Intelligence Oversight Board (IOB) Matter, [redacted] Field Office, IOB Matter 2004-71. (U)

b2
b7E

This LHM sets forth details of investigative activity which the FBI has determined was conducted contrary to The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

DATE: ~~12-03-2030~~
CLASSIFIED BY 65179/DHM/LP/DK
REASON: 1.4 ((C) 05-CV-0845)
DECLASSIFY ON: 12-03-2030

Enclosure

1 - Ms. Thomas
1 - [redacted]
1 - 278-HQ-C1229736-VIO
1 - OPR (IOB 2004-71)
1 - [redacted]

b6
b7C

UNCLASSIFIED WHEN
DETACHED FROM
CLASSIFIED ENCLOSURE

~~Derived from: G-3~~
~~Declassify on: X25-1~~

~~SECRET~~

~~SECRET~~

Mr. James Langdon

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience. (U)

Sincerely,

Julie F. Thomas
Deputy General Counsel

1 - The Honorable Alberto R. Gonzales
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James A. Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

(S)

This matter also has been referred to the FBI's Office of Professional Responsibility for action deemed appropriate. (U)

Derive from: G-3
Declassify on: X25-1
(C)
SECRET

Precedence: ROUTINE Date: 04/29/2004

To: Counterterrorism Attn: ITOS 1/CONUS 1/Team 2
SSA [redacted]
IOS [redacted]
b6
b7C

General Counsel Attn: NSLB/CTLU II
[redacted]

[redacted] Attn: CDC [redacted]
SSA [redacted]
b2
b7E

From: [redacted]
CT-1
Contact: SA [redacted]
b2
b6
b7C

Approved By: [redacted]
b6
b7C

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Case ID #: (U) 278-HQ-C1229736-VIO (Pending)

DATE: 08-30-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-30-2030

Title: (U) PRESIDENTIAL INTELLIGENCE
OVERSIGHT BOARD (IOB)

Synopsis: (U) To report a potential IOB violation involving inadvertent recording of pen/toll information pursuant to the USFISC-authorized installation of a pen register/trap.

~~(SECRET)~~ ~~(U~~ ~~Derived From : G-3~~
~~Declassify On: X1~~

b1 ,b2, b7E

Reference: (U) 66F-HQ-A1247863 Serial 130

Details: ~~(S)~~ Consistent with the guidelines set forth in the referenced communication, [redacted] Division reports that [redacted]

[redacted] (S)

~~(S)~~ [redacted] (S)

~~(S)~~ Controlling legal authority for the relevant investigation is as follows:

b1 , b2, b6, b7C, b7E

---

b1
b2
b6
b7A
b7C
b7E

(S)

(S)

b1 ,b2

[S] authorized on

USFISC-authorized installation of a pen register/trap and trace device was initiated on at by George P. Kazen, Judge, United States Foreign Intelligence Surveillance Court. (U)

b1
b2
b6
b7A
b7C
b7E

(S)

(S)

(S) On approximately SA (case agent) telephoned the Technical Squad and asked to inform

b1
b2
b6
b7C
b7E

(S)

(S)

(S)

(S) On IA noted through

(S)

(S) According to SSA technical

(S)

b1
b2
b6
b7C
b7E

(S)

b1 ,b2, b5, b7E

[redacted] (S)

[redacted] SSA [redacted] subsequently determined that [redacted] (S)

(S) Upon discovering the error [redacted] SA [redacted] immediately notified SSA [redacted] Following the notification to the Technical Squad, SSA [redacted] briefed the appropriate [redacted] Division management personnel and [redacted] SSA [redacted] (S)

b1
b2
b6
b7C
b7E

LEAD(s):

Set Lead 1: (Info)

COUNTERINTELLIGENCE

AT WASHINGTON, DC

(U) SSA [redacted] are requested to coordinate with NSLB to insure that required reporting mandates are met.

b6
b7C

Set Lead 2: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) NSLB is requested to coordinate with ITOS 1/CONUS 1/Team 2 and DOJ/OIPR to ensure required reporting mandates are met.

Precedence: ROUTINE
Date: 02/02/2005

To: Counterterrorism
Attn: ITOS I/CONUS I
SSA [redacted]

b2
b7E
b6
b7C

[redacted] Division
Attn: [redacted]
SSA [redacted]

Inspection Division
Attn: Charlene Thornton

From: General Counsel
National Security Affairs/Room 7975
Contact: [redacted]

b6
b7C

Approved By: Thomas Julie F

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Drafted By: [redacted]

Case ID #: (U) ~~(S)~~ 278-HQ-C1229736-VIO

DATE: 08-30-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-30-2030

Title: (U) ~~(S)~~ UNSUB(s)
COUNTERTERRORISM DIVISION
IOB

Synopsis: (U) ~~(S)~~ It is the opinion of the Office of General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB). OGC will prepare a cover letter and a letterhead memorandum for the General Counsel to report this matter to the IOB.

~~(S)~~ (U) ~~Derived from : G-3~~
~~Declassify on: X-1~~

Reference: (U) ~~(S)~~ 66F-HQ-A1247863-130

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect 8.

b2
b7E

Details: (U) Referenced communication from [redacted] Division to OGC, dated 04/29/04, requested that OGC review the facts of the captioned matter and determine whether it warrants reporting to the IOB. In our opinion, it does. Our analysis follows.

~~(S)~~ As discussed in the referenced electronic communication (EC) and the EC from the Counterterrorism Division ("Counterterrorism") cited below[1], the [redacted] Division initiated a [redacted] (S)

b1
b2
b6
b7A
b7C

(S) The Foreign Intelligence Surveillance Court (FISC) subsequently authorized electronic surveillance (pen register/trap and trace device) was initiated on (S) by George P. Kazen, Judge, United States Foreign Intelligence Surveillance Court).

b1 ,b2, b6, b7A, b7C, b7E

(S) Upon discovering the error on notified the appropriate Counterterrorsim Division authorities.

(U) Section 2.4 of Executive Order (E.O.) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB all information concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive. This language was adopted verbatim from E.O. 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board.

(U) Title 18, United States Code, Section 2511(2)(f) states that the procedures contained in the FISA and Title III of the 1968 Omnibus Crime Control Act (as amended by the Electronic Communications Privacy Act) shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted. Additionally, Section 2.5 of E.O. 12333 provides that, "electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order. Under Title 50, United States Code, Section 1802(b), the FISC is authorized to grant an order approving the electronic surveillance of a foreign power or an agent of a foreign power for the purposes of obtaining foreign intelligence information. Under the pertinent FISA definition, the term electronic surveillance means, the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States. 50 U.S.C. 1801(f)(2).

(S) In this instance, it is clear that as a consequence of an error, the FBI unintentionally obtained electronic data beyond the periods authorized by the FISC. Thus, the surveillance was not authorized under the Foreign Intelligence Surveillance Act or Executive Order 12333. Although steps were taken by FBI [redacted] to sequester the unauthorized take to prevent its use or further dissemination, in accordance with reporting requirements of Section 2.4 of E.O. 12863, FBI [redacted] error nonetheless must be reported to the IOB. OGC will prepare an appropriate cover letter and an LHM for the General Counsel to report this matter to the IOB. b2 b7E

Lead(s):

Set Lead 1: (Action)

COUNTERTERRORISM

AT WASHINGTON, DC

Set Lead 2: (Action)

[redacted]

AT [redacted] b2 b7E

(U) (S) If it has not already been accomplished, coordinate with Counterterrorism Division and FBI [redacted] to ensure that all recordings, log sheets and memoranda of any kind related to the unauthorized ELSUR are collected, sequestered, sealed and delivered to the Counterterrorism Division for submission to the Office of Intelligence Policy and Review, Department of Justice, for destruction.

1 - [redacted] b6 b7C

FOOTNOTES (U)

[1]: (S) EC [redacted] Serial [redacted] from the Counterterrorism Division to Inspection and OGC, dated 05/12/03 and titled "President's Intelligence Oversight Board (PIOB) Matters." b7A

~~SECRET~~

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] DIVISION
FEDERAL BUREAU OF INVESTIGATION HEADQUARTERS (FBIHQ)(U)
2004-55

b2
b7E

Investigation of this IOB matter has revealed that the Division initiated a [redacted] (S)

The Foreign Intelligence Surveillance Court (FISC) subsequently authorized electronic surveillance of [redacted] (S)

Due to an administrative and technical error on the part of FBI [redacted] and [redacted] (S)

A copy of this submission to the IOB has been provided to the FBI's Executive Assistant Director for Counterterrorism/ Counterintelligence. (U)

b1
b2
b6
b7A
b7C
b7E

~~Derived from : G-3~~
~~Declassify on: X1~~

~~SECRET~~

APPROVED:

Director	Crim. Inv.	Inspection	Training
Deputy Director	CJIS	Laboratory	Off. of EEO
	Finance	National Sec.	Affairs
	Gen. Counsel	OPR	Off. of Public &
	Info. Res.	Personnel	Cong. Affs.

Precedence: ROUTINE Date: 02/14/2005

To: [redacted] b2 b7E Attn: SAC
CDC

Counterterrorism Attn: ITOS1/CONUS1
SSA [redacted] b6 b7C

Inspection Attn: SC Toni Fogle

From: General Counsel
National Security Law Branch/LX Crossing Room 5S200
Contact: [redacted]

Approved By: Thomas Julie F
[redacted] b2 b6 b7C

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 09-09-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-09-2030

Case ID #: ~~(S)~~ 278-HQ-C1229736-VIO (Pending)

Title: ~~(S)~~ INTELLIGENCE OVERSIGHT BOARD
(IOB) MATTER 2004-89

Synopsis: ~~(S)~~ It is the opinion of the Office of the General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB)and to the Inspection Division (INSD), FBIHQ. OGC will prepare and deliver the necessary correspondence to the IOB. Our analysis follows.

Reference: ~~(S)~~ 278-HQ-C1229736-VIO Serial 457
278-HQ-C1229736-VIO Serial 555

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in WordPerfect 6.1.

(S) (U) Derived from : G-3
Declassify On: X25-1

Details: (S) As reported by the Counterterrorism Division in an Electronic Communication (EC) dated 09/15/2004, on the division on who are each a United States person as that term is used in Section 101(i) of the Foreign Intelligence Surveillance Act of 1978 (FISA).[1] On obtained authorization from the Foreign Intelligence Surveillance Court (FISC) to install (S)

(S) (S)

(S) On case agent contacted the Technical Squad and advised them that FISA authority would expire on and to disable the line appropriately. Thereafter on Intelligence Analyst (IA) queried Telephone Application and determined that th (S)

(S)

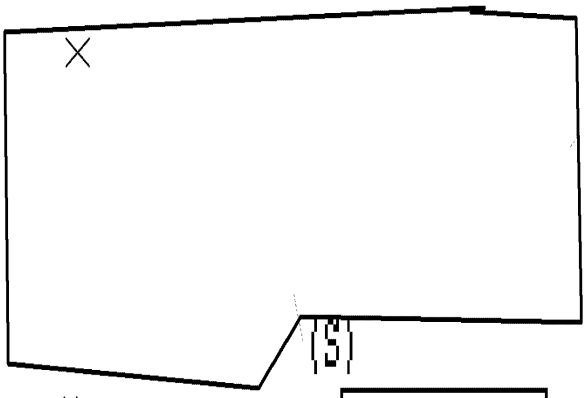
(S) On IA noted through a review of Telephone Applications that the collection (S) The Supervisory Special Agent, Technical Squad, was notified immediately and on that date took the necessary steps to disable the line.

(S) Subsequently it was determined that (S)

b1
b2
b6
b7A
b7C
b7E


(S)
(S)

b1
b2
b7A
b7E


(S)
(S)

(S) Upon discovering the error on [redacted] Case Agent immediately notified the Counterterrorism Squad Supervisor who then briefed the appropriate [redacted] division management and the FBI Headquarters CTD/ITOS 1/CONUS 1/Team 2 Supervisory Special Agent. T[redacted]

b1
b2
b7A
b7E


(S)

(U) (S) Measures have been taken by [redacted] to prevent a recurrence of this error. The Technical Squad's personnel have been instructed in the proper procedures and the need for vigilance in a handling all Court authorized technical surveillance and the need for attentiveness to all aspects of technical collection.

b2
b7E

(U) Section 2-56 of the National Foreign Intelligence Program Manual (NFIPM) requires OGC to determine whether the facts related above are required to be reported to the IOB. Section 2.4 of Executive Order (EO) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB "concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive

order or Presidential directive."

(S) Applying these principles to the case at hand, the OGC concludes that the inadvertent collection of information from the [redacted] (S) was a violation of The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), Section V.14, and the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. 1841-1846. [redacted] (S) When the authorization in the order of the USFISC had expired, further collection on the [redacted] (S) Though the FBI terminated the device in a timely manner, collection was inadvertently reinitiated contrary to the authorization by the US FISC. Consequently, in accordance with E.O. 12863 and Section 2-56 of the NFIPM, the inadvertent error must be reported to the IOB, which this Office will do.

b1
b2
b7A
b7E

LEAD (s):

Set Lead 1: (Info)

[redacted]

AT [redacted]

b2
b7E

(U) Read and Clear.

Set Lead 2: (Action)

INSPECTION

AT WASHINGTON, DC

(U) For action deemed appropriate.

1 - Ms. Thomas
1 - [redacted]
1 - [redacted]
1 - IOB File

b6
b7C

FOOTNOTES (U)

11: (S) A United States person is defined in Section 101(i) of the Foreign Intelligence Surveillance Act (FISA)(codified at 50 U.S.C. 1801 et seq.) as a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . . See also Section I.C of The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG).

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience. (U)

Sincerely,

Julie F. Thomas
Deputy General Counsel

1 - The Honorable Alberto R. Gonzales
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James A. Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

b2
b7E

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
[redacted] FIELD OFFICE
IOB MATTER 2004-89 (U)

b1
b2
b6
b7A
b7C
b7E

Investigation of this IOB matter has determined that on [redacted] the [redacted] Division [redacted] initiated [redacted] who are each a United States person. On [redacted] (S)

obtained authorization from the Foreign Intelligence Surveillance Court (FISC) to [redacted] The [redacted] (S)
residential telephone was serviced by [redacted] which [redacted] (S)
had confirmed that the telephone was subscribed by [redacted] (S)

On [redacted] in accordance with the FISC order, [redacted] discontinued technical surveillance of targets' residential telephone number [redacted] (S)

[redacted] Thereafter on [redacted] a [redacted] (S)
Intelligence Analyst (IA) queried the [redacted]
system and determined [redacted] (S)

On [redacted] IA noted through a review of [redacted] (S)
Supervisory Special Agent, Technical Squad, was notified immediately and on that date took the necessary steps to disable the line. (S)

[redacted] (S)

Derive from: G-3
Declassify on: X25-1

[redacted] (S)

Upon discovering the error on [redacted] appropriate management personnel were notified at [redacted] and at FBI Headquarters. [redacted] (S)

Measures have been taken by [redacted] to prevent a recurrence of this error including instructing [redacted] Technical Squad's personnel in the proper procedures and the need for vigilance in a handling all Court authorized technical surveillance and the need for attentiveness to all aspects of

b1
b2
b6
b7A
b7C
b7E

technical collection. (S) (U)

Though inadvertent, the over collection violated 50 U.S.C. 1842(c)(2) and The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection. (S) (U)

This matter also has been referred to the FBI's Inspection Division for action deemed appropriate. (U)

Precedence: PRIORITY
Date: 01/31/2003

To: Inspection
General Counsel
Counterterrorism
Attn: Inspection Management Unit
National Security Law Unit
RFU

From: [redacted]
Squad 2
Contact: [redacted]
b2
b6
b7C

Approved By: [redacted]
b6
b7C

Drafted By: [redacted] rjg

Case ID #: (U) 278-HQ-C1229736-VIO (Pending)

Title: ~~(S)~~ (U) SA [redacted] INS/JTTF
SSA [redacted]
[redacted] DIVISION
IOB
b2
b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Synopsis: ~~(S)~~ (U) Reporting possible IOB matter

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

DATE: 09-22-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-22-2030

Administrative: ~~(S)~~ (U) Reference telcall on January 24, 2003 between [redacted] Division, and AGC [redacted] OGC FBIHQ.
b1 , b2, b6, b7A, b7C, b7E

Details: ~~(S)~~ On [redacted] the FISA Court, [redacted] (S)

~~(S)~~ On or about [redacted] (S)

~~(S)~~ The [redacted] (S)

b1
b2
b6
b7A
b7C
b7E

however, was not stopped but continued until the expiration of the FISA Court order on [redacted]. Between [redacted] and [redacted] employees, on a weekly basis, [redacted] (S)

(S) This data retrieved [redacted] has been uploaded by [redacted] employees into the [redacted]. The compact disks are presently in elsur storage in [redacted] (S) b1 b2 b7A b7E

(U) (S) [redacted] has reiterated to agents the absolute necessity that they be continuously aware of the status of all elsur coverage on targets.

b2 b7E

LEAD(s):

Set Lead 1: (Adm)

INSPECTION

AT WASHINGTON, DC

(U) (S) Advise [redacted] Division regarding appropriate and necessary future action, especially with respect to compact disks presently in elsur storage. b2 b7E

Set Lead 2: (Adm)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) (S) Advise [redacted] Division with respect to compact disks presently in elsur storage and advise OIPR as appropriate.

Set Lead 3: (Adm) b2 b7E

COUNTERTERRORISM

AT WASHINGTON, DC

(S) Read and clear.
(U)

(01/26/1998)

10BX703.WPD

DATE: 12-12-2005
CLASSIFIED BY 65179 DMH LP CWC
REASON: 1.4 (c)
DECLASSIFY ON: 12-12-2030

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/10/2005

To: Director's Office
Inspection
[redacted] b2 b7E

Attn: OPR
Attn: SSA [redacted]
Attn: SSA [redacted] INS/JTTF
SA [redacted]
SSA [redacted] b6
TTA [redacted] b7C

From: Office of the General Counsel
National Security Law Branch/CILU/Room 7975 b2
Contact: [redacted] b6 b7C

Approved By: Thomas Julie F [redacted]

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Case ID #: (S) 278-HQ-C1229736-VIO
(U) (S) 278-HQ-1415235

Title: (S) (U) SSA [redacted]
SA [redacted] INS/JTTF
SSA [redacted]
TTA [redacted]
[redacted] DIVISION
IOB 2003-27

b2 b6 b7C b7E

Issue handled. Cover loaded in ACS for OPR & IOSD

(U)

Synopsis: (S) It is the opinion of the Office of General Counsel (OGC) that this matter must be reported to the Intelligence Oversight Board (IOB). OGC will prepare and deliver the necessary correspondence to the IOB.

(S)(U) ~~**Derived from : G-3**~~
~~**Declassify On: X1**~~

~~DATE: 09-27-2005~~
~~CLASSIFIED BY 65179/DMH/JW/05-CV-0845~~
~~REASON: 1.4 (C)~~
~~DECLASSIFY ON: 09-27-2030~~

Reference: (S) 278-HQ-1415235 Serial 1
(U)

~~SECRET~~

To: Inspection
From: Office of the General Counsel
Re: (S) (U) 278-HQ-C1229736-VIO, 02/10/2005

Administrative: (U) This communication contains one or more footnotes. To read the footnotes, download and print the document in Corel WordPerfect.

Details: (S) As discussed in the electronic communication (EC)[1] on [redacted] Division initiated a [redacted] who was a "United States person" as that term is used in the then existing Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG)[2] and the Foreign Intelligence Surveillance Act of 1978 (FISA).[3] On [redacted] obtained authority from the Foreign Intelligence Surveillance Court (FISC) to initiate electronic surveillance of subject's [redacted] The initiation and continuation of the FI and the utilization of FISA required that [redacted] comply with the requirements of the FCIG and the FISA. The referenced EC reported that the submission of [redacted] 90-day LHM to National Security Law Unit (NSLU) and the Office of Intelligence Policy and Review (OIPR) was delayed.[4] The 90-day LHM, dated [redacted] was not received by NSLU until [redacted] Further, [redacted] (S)

b1
b2
b7E
b2
b6
b7C
b7E

(U) [1] (S) EC from INSD to OGC and the Director's Office, dated [redacted] and titled "SSA [redacted] [;] SA [redacted] INS/JTTF [;] SSA [redacted] ;] TTA [redacted] Division[;] IOB 2003 27." (INSD EC)

(U) [2] (S) A "United States person" is defined in Section II.W. of the FCIG as "an individual who is. . . [a] United States citizen . . . or . . . [b] a permanent resident alien . . . ." On 10/31/03, the FCIG were superseded by the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). However, because this potential error occurred while the FCIG were in effect, the potential error is analyzed within the context of the then existing FCIG.

[3] (U) The FISA is codified at 50 U.S.C. 1801 et seq. A "United States person" is defined in Section 101(i) of the FISA as: "a citizen of the United States, [or] an alien lawfully admitted for permanent residence ... ."

[4] (U) INSD EC.

[5] (U) These dates were confirmed on [redacted] by Ms. [redacted] National Security Law Unit, Office of the General Counsel. Ms [redacted] maintains a database with the 90-day and annual LHMs submitted on this

b2
b6
b7C

b1
b2
b5
b7E

To: Inspection
From: Office of the General Counsel
Re: (S) 278-HQ-C1229736-VIO, 02/10/2005
(U)

[redacted] (S)

[redacted] Although [redacted] took steps to discontinue monitoring, [redacted]

(U) Section 2.4 of Executive Order (EO) 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, INSD, and the General Counsel, OGC, respectively) report to the IOB concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive. This language was adopted verbatim from EO 12334, dated 12/04/1981, when the IOB was known as the President's Intelligence Oversight Board (PIOB). By longstanding agreement between the FBI and the IOB (and its predecessor, the PIOB), this language has been interpreted to mandate the reporting of any violation of a provision of the FCIG, or other guidelines or regulations approved by the Attorney General in accordance with EO 12333, dated 12/04/1981, if such provisions were specifically intended to ensure the protection of the individual rights of U.S. persons. Violations of provisions that are essentially administrative in nature need not be reported to the IOB. The FBI is required, however, to maintain records of such administrative violations so that the Counsel to the IOB may review them upon request.

(U) (S) As to the first issue of delayed reporting, Section IX of the FCIG set forth rules governing

---

subject.

[6] (U) INSD EC. It is unclear from the EC submitted whether [redacted] appropriately sequestered the materials related to the [redacted] If it has not been already accomplished, the sequestered materials must be submitted, [redacted]

b2
b5
b7E

To: Inspection
From: Office of the General Counsel
Re: (S) 278-HQ-C1229736-VIO, 02/10/2005

(U)

the reporting of information concerning foreign counterintelligence and international terrorism investigations. Section IX.C provided in pertinent part that:

> Each full investigation of any U.S. person **shall be reported within ninety (90) days of initiation** to the Office of Intelligence Policy and Review, setting forth the basis for undertaking the investigation. The FBI shall furnish to the Attorney General or a designee **a summary of each investigation at the end of each year the investigation continues**, including specific information on any requests for assistance made by the FBI to foreign law enforcement, intelligence or security agencies. (Emphasis added.)

(U) (S) Section IX.C was intended to regulate the timely reporting of FBI full investigations on U.S. persons to the OIPR. As such, it was written to include both administrative and "rights protection" components. The 90-day and annual reporting requirements of Section IX.C are purely administrative in nature, while the oversight exercised by the OIPR in reviewing the required reporting ensures the protection of individual rights. As a general rule, delinquent annual or 90-day LHMs are considered to be violations of an administrative nature when they are submitted to the NSLU within 90 days of their original due date. These administrative violations are placed in the control file for periodic review by the Counsel to the IOB. When an LHM is not submitted at all, or is submitted later than 90 days from its original due date, the facts and circumstances of that particular case must be examined to determine whether the failure or substantial delay in submitting the LHM precluded meaningful oversight and review by the OIPR. If OIPR was precluded from conducting such oversight and review, then the matter must be reported to the IOB.

(U) (S) As previously discussed, [redacted] 90-day LHM, dated [redacted] was not received by NSLU until [redacted] Although delayed, because the delay was less then 90 days, the

b2
b7E

To: Inspection
From: Office of the General Counsel
Re: (S) 278-HQ-C1229736-VIO, 02/10/2005

(U)

error is considered to be of administrative nature. Accordingly, the delayed submission of the 90-day LHM is not reportable to the IOB. A record of this decision should be maintained in the control file for future review by Counsel to the IOB.

(U) (S) As to the second issue of [redacted] Section 2.5 of Executive order 12333 provides that: "[e]lectronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act ... ." Each request for the issuance of a FISC order for the pen register and trap and trace surveillance is supported by an application. As required by the FISA, requestor of the FISA provided a certification "that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."[7]

b2
b5
b7E

(U) (S) As previously discussed [redacted] This action was contrary to the Executive order 12333 and the FISA. Consequently, in accordance with the reporting requirements of Section 2.4 of E.O. 12863, OGC will prepare a correspondence to report this matter to the IOB.

b2
b5
b7E

[7] (U) 50 U.S.C. 1842, Section 402(c)(2).

To: Inspection
From: Office of the General Counsel
Re: (S) (U) 278-HQ-C1229736-VIO, 02/10/2005

LEAD (s):

Set Lead 1: (Action)

DIRECTOR'S OFFICE

AT OPR FO, DC

(U) For action deemed appropriate.

Set Lead 2: (Action)

INSPECTION

AT WASHINGTON, DC

(U) For action deemed appropriate.

Set Lead 3: (Action)

b2
b5
b7E

[redacted]

[redacted]

(S) (U) If it has not already been accomplished, [redacted]

[redacted]

CC: Ms. Thomas

To: Inspection
From: Office of the General Counsel
Re: (S) 278-HQ-C1229736-VIO, 02/10/2005

(U)

[redacted] b6 b7C

IOB Library

♦♦

Precedence: PRIORITY Date: 09/13/2004

To: General Counsel Attn: NSLB
CTLU I

From:
CDC
Contact:

Approved By:

Drafted By:

Case ID #: (U) 278-HQ-C1229736
(U) 278- 75423

Title: (U) SSA
SA
INTELLIGENCE OVERSIGHT BOARD MATTERS

DATE: 12-12-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-12-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2
b6
b7C
b7E

(U) RESTRICTED DOCUMENT - DISSEMINATE TO PERSON(S) WITH ROLE

Synopsis: (U) This communication brings captioned matter to the attention of FBIHQ, Office of the General Counsel (OGC).

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) b7A

Details: (U) SUMMARY

(U) ~~(S)~~

(U) ~~(S)~~

b2
b5
b7A
b7E

b2
b5
b7E

(U) DETAILS

b1
b2
b5
b6
b7A
b7C
b7E

(S)

(S)

(S/NF/OC) According to Telecommunications Specialist and Special Agent (SA) Technically Trained Agent (TTA), three FBI employees re-checked the wiring and programming of the FBI's equipment and everything was done correctly. Telecommunications Unit (TU

(S)

(S/NF/OC) On SA TTA went to the box where the FBI had

(S)

(S/NF/OC)

(S)

b1 ,b2, b5, b6, b7A, b7C, b7E

b1
b2
b5
b7A
b7E

[redacted] (S)

b1
b2
b5
b6
b7A
b7C
b7E

[redacted] (S)

(U) SA [redacted] has previously notified the Department of Justice, Office of Intelligence Policy and Review (DOJ OIPR) concerning this matter.

b6
b7C

(U) SAC RECOMMENDATIONS:

(U) (S) SAC [redacted] recommends no administrative or disciplinary action occur in this matter. The employees involved in this matter did not intentionally intercept the data and took continuing and exhaustive steps to find the reason for the error and correct it. Even in the face of correctly connected machinery and repeated assertions by the telecommunications provider that there was no error, the employees continued to search for the reason for the apparent mistake. SAC, [redacted] believes the [redacted] personnel involved in this matter acted appropriately and commends them for their tenacity in rooting out the telecommunication service provider's mistake.

b2
b7E

LEAD(s):

Set Lead 1: (Action)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) At NSLB, CTLU I, please review the cricumstances described herein and advise [redacted] Division as to your findings.

b2
b7E

Precedence: PRIORITY Date: 03/22/2005

To: [redacted] Attn: SAC
CDC

Counterterrorism Attn: ITOS I / CONUS IV
SSA [redacted]

Inspection Attn: IIS
SC [redacted]

b2
b6
b7C
b7E

From: General Counsel
NSLB/CTLU I/Room 7975
Contact: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Approved By: Thomas Julie F
[redacted]

b6
b7C

Drafted By: [redacted]

DATE: 09-27-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-27-2030

Case ID #: (U) 278-HQ-C1229736 (Pending)
(U) 278 [redacted] 75423 (Pending)

b2
b7E

Title: (U) SSA [redacted]
SA [redacted]
INTELLIGENCE OVERSIGHT BOARD MATTER
(U) IOB 2004-85

Synopsis: ~~(S)~~ It is the opinion of the Office of General Counsel (OGC) that the above referenced matter must be reported to the Intelligence Oversight Board (IOB) and to the FBI Inspection Division, Internal Investigations Section. Our analysis follows.

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

[redacted] b6 b7C

Reference: (S) 278-HQ-C1229736 Serial 1904 b2
(U) (S) 278 75423 Serial 47 b7E
(S)

Details: (S) Pursuant to Foreign Intelligence Surveillance Court (FISC) order Division (hereinafter received authority for a Pen Register/Trap & Trace (PR/TT) for facilities a subject of an investigation under file number (S) a U.S. person (USPER), as that term is used in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG or the Guidelines).[1] The order authorized the PR/TT to begin on and it was to be terminated on (S)

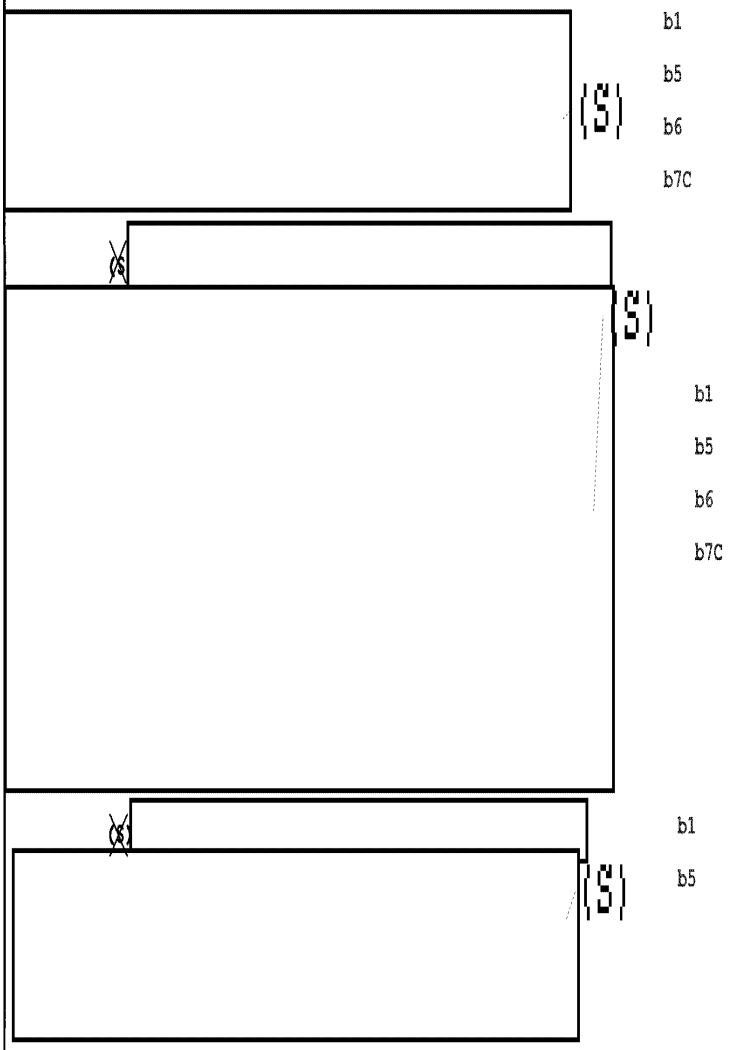
b1
b2
b5
b6
b7A
b7C
b7E

(S) (S) Pursuant to another FISC order was authorized to begin full conten an USPER being investigated under file number (S) (S)

b1
b2
b5
b7A
b7E

(S)

b1
b6
b5
b7C



b1
b5
b6
b7C
(S)
(S)
b1
b5
b6
b7C
(S)
(S)
b1
b5

(U) (S) Consistent with the requirements of Executive Order (E.O.) 12863 and Section 2-56 of the National Foreign Intelligence Program Manual (NFIPM), OGC was tasked to determine whether the surveillance error described here is a matter which must be reported to the IOB. We conclude that it must. Section 2.4 of E.O. 12863, dated 09/13/1993, mandates that Inspectors General and General Counsel of the Intelligence Community components (in the FBI, the Assistant Director, Inspection Division, and the General Counsel, OGC, respectively) report to the IOB all information concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

(U) Title 18, United States Code, Section 2511(2)(f) states that the procedures contained in the FISA and Title III of

the 1968 Omnibus Crime Control Act (as amended by the Electronic Communications Privacy Act) shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted. Additionally, Section 2.5 of E.O. 12333 provides that, ïe´lectronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order. Under Title 50, United States Code, Section 1802(b), the FISC is authorized to grant an order approving the electronic surveillance of a foreign power or an agent of a foreign power for the purposes of obtaining foreign intelligence information. Under the pertinent FISA definition, the term electronic surveillance means, the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States... 50 U.S.C. 1801(f)(2).

(U) ~~(S)~~ In this instance, it is clear that as a consequence of an error on the part of a communications carrier, [redacted] the FISC. Even thoug[redacted] was diligent in its discovery of the [redacted] the Foreign Intelligence Surveillance Act or Executive Order 12333. Consequently, in accordance with E.O. 12863 and Section 2-56 of the NFIPM, [redacted] to the IOB, which this Office will do. OGC will prepare an appropriate cover letter and an LHM for the Deputy General Counsel to report this matter to the IOB.

b2
b5
b7E

FOOTNOTES (U)

ï1´: ~~(S)~~ A United States person is defined in section II.W of the Guidelines as an individual who is . . . ïa´ United States citizen

. . .

or . . . a permanent resident alien . . . . This regulatory definition is based on the definition of a United States person as that term is used section 101(i) of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801 et seq. The latter states, in pertinent part, that a United States person means a citizen of the United States or an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Naturalization Act) . . . .

LEAD(s):

Set Lead 1: (Discretionary)

[redacted]

AT [redacted]

(U) (X) Coordinate with FBIHQ, the Counterterrorism Division, ITOS I, CONUS IV, to ensure that [redacted] are collected, sequestered, sealed and delivered to CONUS IV for submission to the Office of Intelligence Policy and Review, Department of Justice, for destruction.

b2
b5
b7E

Set Lead 2: (Discretionary)

INSPECTION

AT WASHINGTON, DC

(U) For appropriate action.

Set Lead 3: (Info)

COUNTERTERRORISM

AT WASHINTON, D.C.

(U) For information only.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 10-05-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 10-05-2030

BY COURIER

Mr. James Langdon
Chairman
Intelligence Oversight Board
Room 5020
New Executive Office Building
725 17th Street, N.W.
Washington, D.C. 20503

Dear General Scowcroft:

This letter forwards for your information a self-explanatory enclosure entitled, "Intelligence Oversight Board (IOB) Matter, IOB 2004-85." (U)

The enclosure sets forth details of investigative activity which the FBI has determined may have been contrary to the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and/or laws, Executive Orders, or Presidential Directives which govern FBI foreign counterintelligence and international terrorism investigations. (U)

1 - Ms. Thomas
1 - [redacted]
1 - [redacted]
1 - IOB Library
1 - 278-HQ-C1229736-VIO

b6
b7C

~~UNCLASSIFIED WHEN DETACHED FROM CLASSIFIED ENCLOSURE~~

[redacted]

b6
b7C

Should you or any member of your staff require additional information concerning this matter, an oral briefing will be arranged for you at your convenience.

Sincerely,

Julie Thomas
Deputy General Counsel

Enclosure

1 - The Honorable Alberto R. Gonzalez
Attorney General
U.S. Department of Justice
Room 5111

1 - Mr. James Baker
Counsel, Office of Intelligence Policy and Review
U.S. Department of Justice
Room 6150

INTELLIGENCE OVERSIGHT BOARD (IOB) MATTER
IOB 2004-85 (U)

b2
b5
b7E

~~(S)~~ [redacted] As a result of this [redacted] instead of capturing the telephone communications of another

subject who was actually the target of the order issued by the Foreign Intelligence Surveillance Court (FISC).

(S)

(S)

b1 , b5, b6, b7C

(S)

The matter is therefore reportable to the Intelligence Oversight Board under the terms of Executive Order 12863. In addition, it has been referred to the FBI's Inspection Division, Internal Investigations Section for any action that is deemed appropriate.

~~SECRET~~

b1 ,b5, b6, b7C

~~Derived from: G-3~~
~~Declassify on: X-1~~

~~UNCLASSIFIED WHEN~~
~~DETACHED FROM~~
~~CLASSIFIED ENCLOSURE~~

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 3
Page 119 ~ Duplicate
Page 120 ~ Duplicate
Page 121 ~ Duplicate

THOMAS, JULIE F. (OGC) (FBI)

From: Caproni, Valerie E. (OGC) (FBI)
Sent: Monday, November 29, 2004 12:04 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: Combined Business Record/Pen Register

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-08-2005 BY 65179/DMH/LP/RW 05-CV-0845

b5

[redacted]

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 29, 2004 11:59 AM
To: Caproni, Valerie E. (OGC) (FBI)
Subject: Combined Business Record/Pen Register

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Dear Valerie,

[redacted]

b5
b6
b7C

Julie F. Thomas
DGC, National Security Law Branch
Office of the General Counsel
Room 7975
[redacted]
Julie.Thomas@ic.fbi.gov

b2

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted] (OGC) (OGA) b6 b7C
Sent: Monday, November 29, 2004 11:38 AM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: Pen Register

DATE: 12-12-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-12-2030

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

thanks Julie. [redacted] b5 b6 b7C

Valerie [redacted]

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 29, 2004 10:18 AM
To: [redacted] (OGC) (OGA) b6 b7C
Subject: FW: Pen Register

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

[redacted] Julie b6 b7C b5

-----Original Message-----
From [redacted] (ITD) (FBI)
Sent: Monday, November 29, 2004 9:56 AM
To [redacted] (ITD) (FBI); [redacted] (ITD) (FBI) b6 b7C
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: Pen Register

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

Deputy General Counsel Thomas, b5 b6 b7C

[redacted]

Sorry for the delay.

SSA [redacted] b6 b7C b2

-----Original Message-----
From [redacted] (ITD) (FBI) b6
Sent: Monday, November 08, 2004 2:25 PM b7C
To [redacted] (ITD) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Pen Register Fax

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

(S)

b1
b6
b7C
b5

Deputy General Counsel Julie Thomas

b6
b7C
b2

-----Original Message-----
From: (ITD) (FBI)
Sent: Monday, November 08, 2004 2:02 PM
To: (ITD) (FBI); ITD) (FBI)
Subject: Pen Register Fax

b6
b7C

~~SECRET~~
RECORD 268-hq-1092598-K

see attached.

~~DERIVED FROM: Single Source Document~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Single Source Document~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Single Source Document~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Single Source Document~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Single Source Document~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 29, 2004 12:06 PM
To: [redacted] (OGC) (OGA)
Subject: RE: Pen Register

b6
b7C

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

[redacted] Valerie. [redacted] Thanks, Julie

b6
b7C
b5

-----Original Message-----
From [redacted] (OGC) (OGA)
Sent: Monday, November 29, 2004 11:38 AM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: Pen Register

DATE: 12-12-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-12-2030

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

thanks Julie. [redacted] Spike [redacted] Valerie [redacted]

b6
b7C
b5

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 29, 2004 10:18 AM
To: [redacted] (OGC) (OGA)
Subject: FW: Pen Register

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

[redacted] Thanks, Julie

-----Original Message-----
From [redacted] (ITD) (FBI)
Sent: Monday, November 29, 2004 9:56 AM
To [redacted] (ITD) (FBI); [redacted] ITD) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: Pen Register

b6
b7C
b5

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

Deputy General Counsel Thomas,

[redacted]

b6
b7C
b5

SSA [redacted] b6 b7C b2

-----Original Message-----
From [redacted] (ITD) (FBI)
Sent: Monday, November 08, 2004 2:25 PM
To: [redacted] (ITD) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Pen Register Fax

b1 b6 b7C

SECRET (U) (S)
RECORD 268-hq-1092598-K

[redacted] Deputy General Counsel Julie Thomas [redacted]

[redacted]

[redacted]

b6 b7C b2

-----Original Message-----
From: [redacted] (ITD) (FBI)
Sent: Monday, November 08, 2004 2:02 PM
To: [redacted] (ITD) (FBI); [redacted] (ITD) (FBI)
Subject: Pen Register Fax

b6 b7C

SECRET
RECORD 268-hq-1092598-K

see attached.

DERIVED FROM: Single Source Document
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: Single Source Document
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: Single Source Document
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: Single Source Document

DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: Single Source Document
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: Single Source Document
DECLASSIFICATION EXEMPTION 1
SECRET

THOMAS, JULIE F. (OGC) (FBI)

b6
b7C

From: [redacted](ITD) (FBI)
Sent: Monday, November 08, 2004 2:25 PM
To: [redacted](ITD) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Pen Register Fax

DATE: 12-12-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-12-2030

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

[redacted] Deputy General Counsel Julie Thomas [redacted] (S)

[redacted] (S)

b6
b7C
b1
b2
b7E
b5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted](ITD) (FBI)
Sent: Monday, November 08, 2004 2:02 PM
To: [redacted](ITD) (FBI) [redacted](ITD) (FBI)
Subject: Pen Register Fax

b6
b7C

~~SECRET~~ (U)
RECORD 268-hq-1092598-K

see attached.

Need by Friday

~~DERIVED FROM: Single Source Document~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Single Source Document~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 08, 2004 3:33 PM
To: [redacted] (OGC) (OGA) b6 b7C
Subject: Delegations

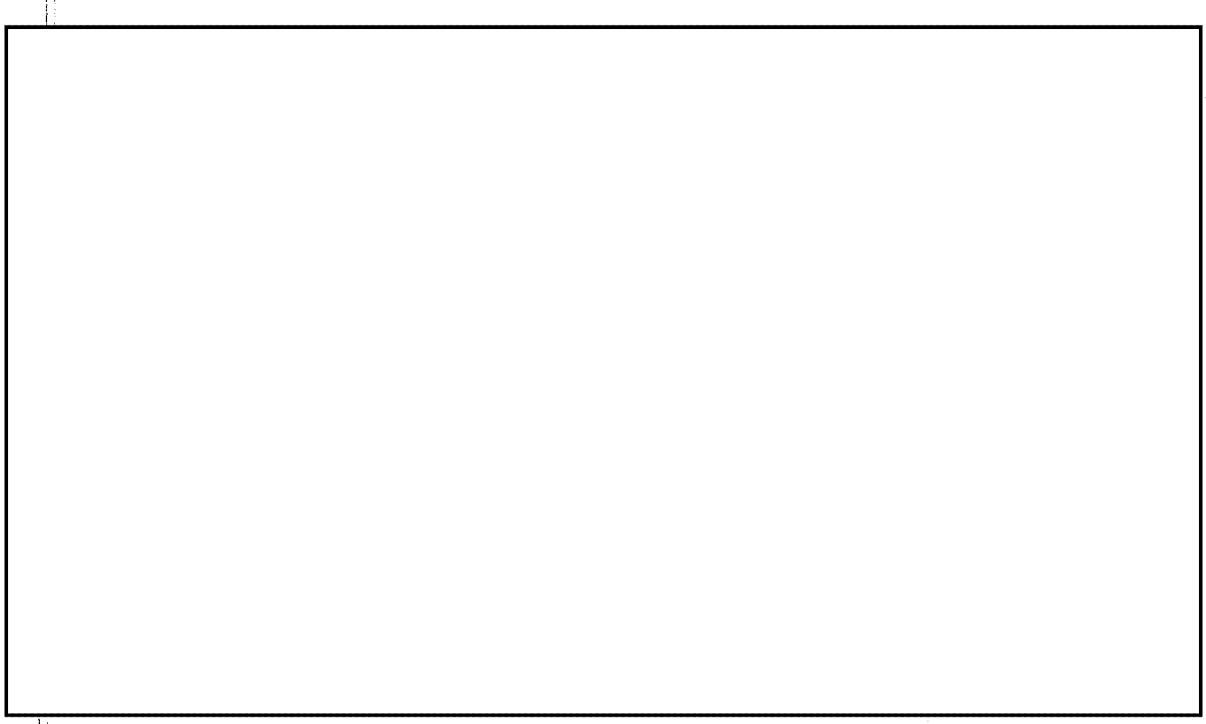
UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

On October 10, 2003, the authority to approve an application for business records was delegated by the Director to the Deputy Director, the EAD for Counterterrorism/Counterintelligence, the AD and all DADs of the Counterterrorism, Counterintelligence, and Cyber Divisions, the General Counsel, the Deputy General Counsel for National Security Affairs (me) and the Senior Counsel for National Security Affairs (Spike). [redacted] b5 b2

Julie Thomas
[redacted]

UNCLASSIFIED



b2
b5
b6
b7C

THOMAS, JULIE F. (OGC) (FBI) b6 b7C

From: [redacted] (OGC) (FBI)
Sent: Thursday, October 21, 2004 11:02 AM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW:

b5 b6 b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie: [redacted]

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, October 15, 2004 12:53 PM
To: [redacted] (OGC) (FBI)
Subject:

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE b6 b7C

SECRET

This is the information I propose to give to Julie about business records:

[redacted] b5

b5

(S)

b1

(S)

b1
b2
b7E

b5

[redacted] b5

SENSITIVE BUT UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI) b6 b7C

From: [redacted] (OGC) (FBI)
Sent: Thursday, October 21, 2004 11:20 AM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: [redacted] equest

DATE: 12-12-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-12-2030

(S) b1

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie,

[redacted] b5

(S) b1

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI) b6
Sent: Thursday, October 21, 2004 11:03 AM b7C
To: [redacted] (OGC) (FBI)
Subject: RE:

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I have forwarded to Julie. Thanks.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted] (OGC) (FBI) b6
Sent: Friday, October 15, 2004 12:53 PM b7C
To: [redacted] (OGC) (FBI)
Subject:

SECRET

This is the information I propose to give to Julie about business records:

[redacted] b5

SECRET

b5

b5

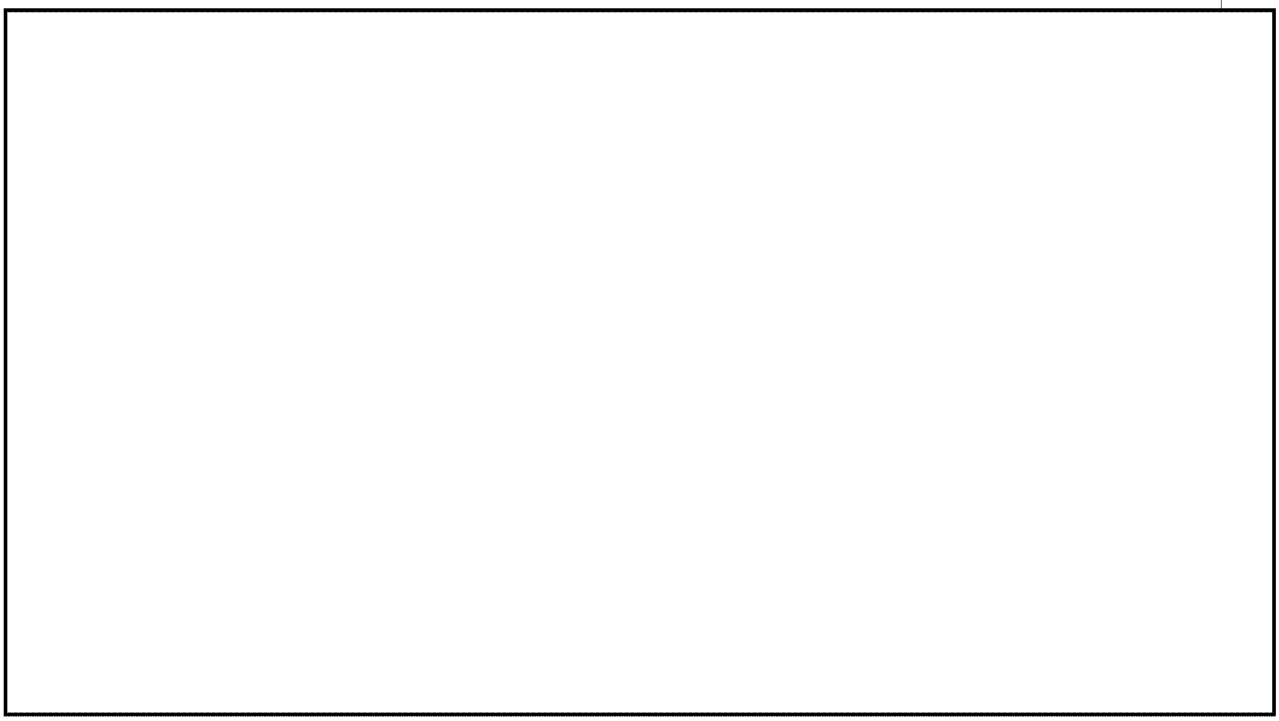
(S)

b1

(S)

b1
b2
b7E

b5



b5

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, October 14, 2004 2:23 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: FW: Iraqi Insurgency Pleading

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-12-2005 BY 65179/DMH/LP/RW 05-cv-0845

SECRET

Julie --

[redacted]

FYI -
[redacted] Spike [redacted]
[redacted] Spike [redacted]

[redacted]

b5

[redacted]

b5
b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, October 14, 2004 1:10 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (CTD) (FBI); [redacted] (CTD) (FBI); [redacted] (OGC) (FBI)
Subject: Iraqi Insurgency Pleading

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

SECRET

Spike, [redacted]

[redacted]

[redacted]

b5

[redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Friday, October 22, 2004 1:06 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: business records

DATE: 12-12-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-12-2030

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Here is a copy of the powerpoint on national security letters, business records, etc.

[redacted]

(S)

b1
b2
b7E
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SECRET

FISA - Business Records

SECRET

SECRET

- Patriot Act expanded universe of items obtainable, to "any tangible things (including books, records, papers, documents and other items)"
- Patriot Act changed legal standard: "the information to be obtained is foreign intelligence information not concerning a US person , or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence gathering activities" and investigation of USP cannot be based solely on activities protected by First Amendment
- Same standard as established by Patriot Act for PR/TT; NSLs
- Available in PI and full investigations

FISA - Business Records

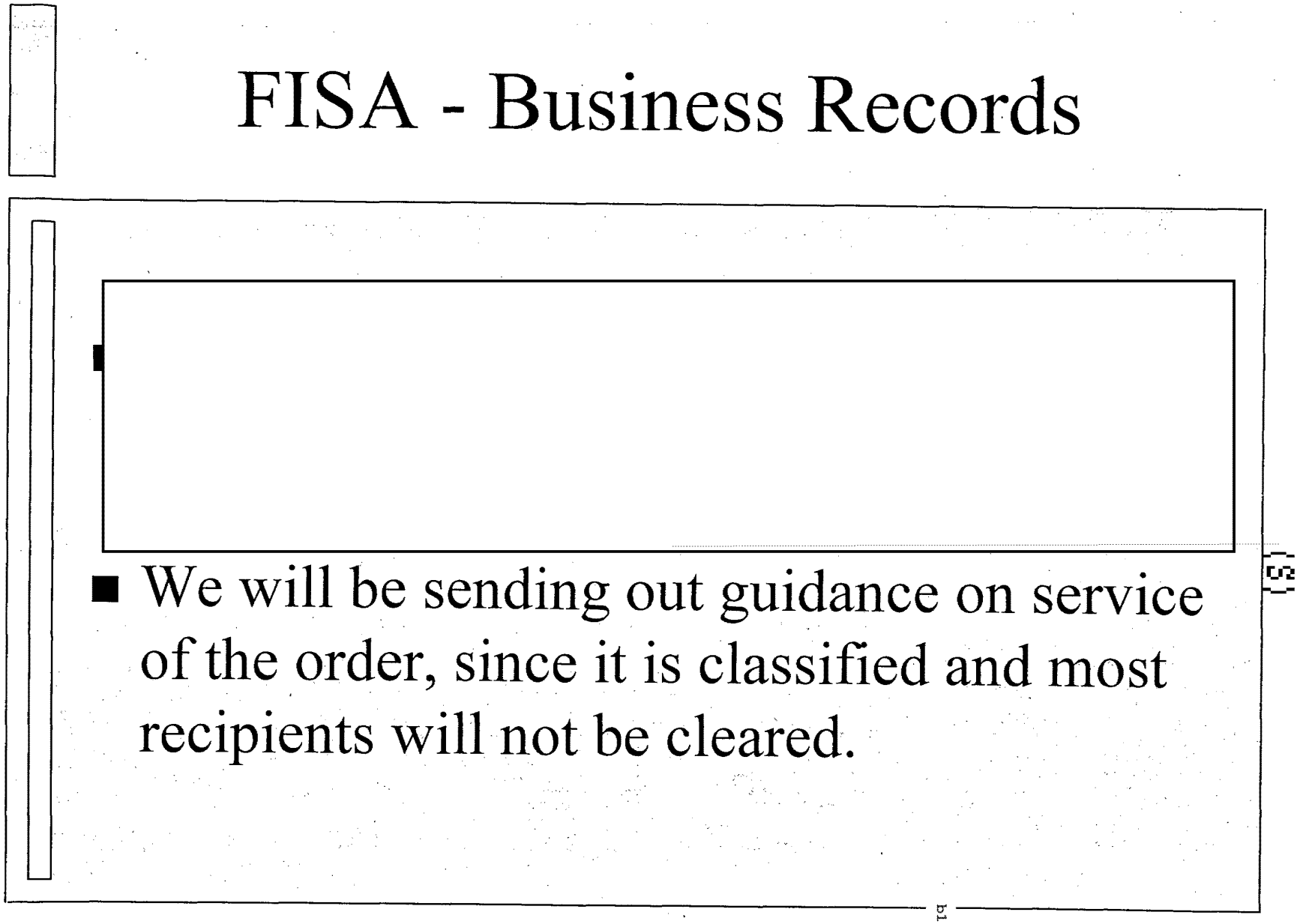
SECRET

SECRET

- FISA permits delegation down to level of ASAC
- At current time, approval authority has been delegated to headquarters officials (Deputy Director; EAD for CT/CI; AD and all DADs of CT, CI, Cyber; General Counsel, Deputy General Counsel for National Security Affairs, and Senior Counsel for National Security Affairs)
- Business records form available for field to fill out and submit to headquarters and NSLB (atty

b6
b7C

FISA - Business Records



- We will be sending out guidance on service of the order, since it is classified and most recipients will not be cleared.

[redacted] (OGC) (FBI) b6 b7C

From: [redacted] (OGC) (FBI)
Sent: Wednesday, November 10, 2004 1:46 PM
To: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: [redacted] quest (S)

b6 b7C

DATE: 12-12-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-12-2030

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S)

[redacted] b1 b2 b7E

[redacted] (S)

All in all, I guess we should go along with this. But this is no longer an FBI document, it's an OIPR document, and I don't like that fact.

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Although I haven't broached the subject with OIPR since Julie's discussion with Baker, it appears from the fact that we have copies that OIPR says are ready to go indicates [redacted] b5 b6 b7C

[redacted]

SENSITIVE BUT UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 136
Page 2 ~ Referral/Direct
Page 3 ~ Referral/Direct
Page 4 ~ Referral/Direct
Page 5 ~ Referral/Direct
Page 6 ~ Referral/Direct
Page 7 ~ Referral/Direct
Page 8 ~ Referral/Direct
Page 9 ~ Referral/Direct
Page 10 ~ Referral/Direct
Page 11 ~ Referral/Direct
Page 21 ~ Referral/Direct
Page 22 ~ Referral/Direct
Page 23 ~ Referral/Direct
Page 24 ~ Referral/Direct
Page 25 ~ Referral/Direct
Page 26 ~ Referral/Direct
Page 27 ~ Referral/Direct
Page 28 ~ Referral/Direct
Page 29 ~ Referral/Direct
Page 30 ~ Referral/Direct
Page 31 ~ Referral/Direct
Page 32 ~ Referral/Direct
Page 33 ~ Referral/Direct
Page 34 ~ Referral/Direct
Page 35 ~ Referral/Direct
Page 36 ~ Referral/Direct
Page 37 ~ Referral/Direct
Page 38 ~ Referral/Direct
Page 39 ~ Referral/Direct
Page 40 ~ Referral/Direct
Page 41 ~ Referral/Direct
Page 42 ~ Referral/Direct
Page 43 ~ Referral/Direct
Page 44 ~ Referral/Direct
Page 45 ~ Referral/Direct
Page 46 ~ Referral/Direct
Page 47 ~ Referral/Direct
Page 48 ~ Referral/Direct
Page 49 ~ Referral/Direct
Page 50 ~ Referral/Direct
Page 51 ~ Referral/Direct
Page 52 ~ Referral/Direct
Page 53 ~ Referral/Direct
Page 54 ~ Referral/Direct

Page 55 ~ Referral/Direct
Page 56 ~ Referral/Direct
Page 57 ~ Referral/Direct
Page 58 ~ Referral/Direct
Page 59 ~ Referral/Direct
Page 60 ~ Referral/Direct
Page 61 ~ Referral/Direct
Page 65 ~ Referral/Direct
Page 66 ~ Referral/Direct
Page 67 ~ Referral/Direct
Page 68 ~ Referral/Direct
Page 69 ~ Referral/Direct
Page 70 ~ Referral/Direct
Page 71 ~ Referral/Direct
Page 72 ~ Referral/Direct
Page 73 ~ Duplicate
Page 74 ~ Duplicate
Page 75 ~ Duplicate
Page 76 ~ Duplicate
Page 77 ~ Duplicate
Page 78 ~ Duplicate
Page 79 ~ Duplicate
Page 106 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 128 ~ Referral/Direct
Page 129 ~ Referral/Direct
Page 130 ~ Referral/Direct
Page 131 ~ Referral/Direct
Page 132 ~ Referral/Direct
Page 133 ~ Referral/Direct
Page 134 ~ Referral/Direct
Page 135 ~ Referral/Direct
Page 136 ~ Duplicate
Page 137 ~ Referral/Direct
Page 138 ~ Referral/Direct
Page 139 ~ Referral/Direct
Page 140 ~ Referral/Direct
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Referral/Direct
Page 145 ~ Referral/Direct
Page 147 ~ Duplicate
Page 148 ~ Duplicate
Page 149 ~ Duplicate
Page 150 ~ Duplicate
Page 151 ~ Duplicate
Page 152 ~ Duplicate

Page 153 ~ Duplicate
Page 154 ~ Duplicate
Page 155 ~ Duplicate
Page 156 ~ Duplicate
Page 157 ~ Duplicate
Page 158 ~ Duplicate
Page 159 ~ Duplicate
Page 160 ~ Duplicate
Page 161 ~ Duplicate
Page 162 ~ Duplicate
Page 163 ~ Duplicate
Page 164 ~ Duplicate
Page 165 ~ Duplicate
Page 166 ~ Duplicate
Page 167 ~ Duplicate
Page 168 ~ Duplicate
Page 169 ~ Duplicate
Page 170 ~ Duplicate
Page 171 ~ Duplicate
Page 172 ~ Duplicate
Page 173 ~ Duplicate
Page 174 ~ Referral/Direct
Page 175 ~ Referral/Direct
Page 176 ~ Referral/Direct
Page 177 ~ Referral/Direct
Page 178 ~ Referral/Direct
Page 179 ~ Referral/Direct
Page 180 ~ Referral/Direct
Page 181 ~ Referral/Direct
Page 182 ~ Referral/Direct
Page 183 ~ Referral/Direct
Page 184 ~ Referral/Direct
Page 185 ~ Referral/Direct
Page 186 ~ Referral/Direct
Page 187 ~ Referral/Direct
Page 188 ~ Referral/Direct
Page 189 ~ Referral/Direct
Page 190 ~ Referral/Direct
Page 191 ~ Referral/Direct
Page 192 ~ Referral/Direct
Page 193 ~ Referral/Direct

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Uploaded 10/10/03

Precedence: IMMEDIATE **Date:** 09/12/2003

To: All Divisions **Attn:** ADIC, AD, DAD, SAC, CDC

From: Office of the General Counsel
National Security Law Branch
Contact: [redacted] b2 b6 b7C

Approved By: Mueller Robert S III

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-08-2005 BY 65179/DMH/LP/RW 05-cv-0845

Case ID #: 66F-HQ-A1431182 Serial 2

Title: BUSINESS RECORD APPLICATIONS
DELEGATION OF AUTHORITY

Synopsis: Delegates signature authority for Applications for Business Records to FBIHQ officials under 50 U.S.C. § 1861.

Details: The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C § 1861, provides for access to certain business records for foreign intelligence (FI) and international terroris (IT) investigations through issuance of an order from the FISA Court (FISC). Section 1861(a) authorizes the "Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge)" to make an application for the order.

Thus, as permitted by 50 U.S.C. § 1861(a), I hereby designate certification signature authority for applications for FISA business records to the following FBI Officials:

1. The Deputy Director;

2. The Executive Assistant Director for Counterterrorism/Counterintelligence;

3. The Assistant Director and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; and

4. The General Counsel, the Deputy General Counsel for National Security Affairs, and the Senior Counsel for National Security Affairs.

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ-A1431182, 07/18/2003

The National Security Law Branch is hereby authorized to prepare business record applications and will issue guidance on the application process.

LEAD:

Set Lead 1: (adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in CI and IT operations and to other personnel as appropriate.

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE HEARING
NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?

b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors.

[redacted] b5

For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?

b5

b5

b5

b5

How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

b5

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing.

b5

b5 which account for approximately 75% of the total FISAs for the FBI. The remaining FBI field offices are in the process of being trained on the FISAMS. [redacted]

High Performance Technologies, Inc.(HPTi) is the contractor for the development of the FISAMS. During FY 2003, we currently have allocated $900,000 for Version 1.0 of the FISAMS. We are contracting an additional $1 million with HPTi for enhancements beginning September 2004, which was funded by the Wartime Supplemental Funds received by the FBI. There will be several follow-up versions to further enhance the FISAMS in the future.

b5 [redacted] FY06 is the first budget cycle the FISA Unit has been able to formally request funding for this project.

59. OGC. (Follow-up to Leahy 18C) Did you personally review the 4 FISA applications reportedly not approved by the FISA court last year? Can you provide any details on why the 4 applications were not approved?

b5 [redacted]

60. OGC. (Follow-up to Leahy 18D) Can you provide us with a blank copy of the FISA Request Form referenced in your response? Will you provide us with a blank copy of the form that the FBI created for requesting business records from the FISA court?

b5 [redacted]

b5

61. OGC. (Follow-up to Leahy 21) Did you refer the question to DOJ OIPR? When? Have you been asked to assist in the response? When?

OCA Note: OCA proposes to respond that the FBI forwarded its responses to DOJ on 10/22/03, including our indication that the answer to Senator Leahy's question 21 called for classified information, which is ordinarily supplied to Congress by DOJ's Office of Intelligence Policy and Review (OIPR). By letter to the Committee dated 3/4/04, DOJ's Office of Legislative Affairs forwarded the Department's responses to the Committee, including the FBI's original response to this question.

Response: OGC concurs with OCA's response.

74. CTD. In June 2003, Glenn Fine, the Inspector General for the Justice Department, found "significant problems in the way the detainees were handled" following 9/11. These problems included a failure by the FBI to distinguish between detainees whom it suspected of having a connection to terrorism and detainees with no connection to terrorism; the inhumane treatment of the detainees at a federal detention center in Brooklyn; and the unnecessarily prolonged detention resulting from the Department's "hold until cleared" policy - made worse by the FBI's failure to give sufficient priority to carrying out clearance investigations. In your opinion, has the Justice Department responded in an appropriate manner to all the abuses identified in the Inspector General's report? What steps has the FBI taken to prevent such abuses from occurring in the future?

b5

[redacted]

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response: This information may be disseminated in any format deemed appropriate for the particular circumstances. [redacted]

b5

[redacted]

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been

issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

b5

[redacted] b5

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: [redacted] b5 [redacted] **OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information. [Note: DOJ has provided or is in the process of providing examples of how the Patriot Act has been an asset to our investigations and why the sunset provisions should not sunset. We refer OCA to the DOJ for these examples.]**

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

b5 [redacted]

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one.

b2
b7E
b5

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community,

b5 through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins.

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence.

b5 Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism

Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners,

b5 In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, access and responsiveness to local FBI field office, FBI program and national intelligence requirements . The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during

the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

[redacted] b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

b5

[redacted]

(i) How many of such cases were terrorism-related?

[redacted]

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application

of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation

received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b1
b7A
b5

Response:

(S)

b5

(S) (U)

b5

(U)

b5

b5

b5

(U)

(U)

(S)

(S)

(S)

b1

b5

b5

b5 [redacted]

b5 [redacted]

b5 [redacted]

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation

of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b5

b5

~~SECRET~~

b5

(S)

(S)

b1
b5
b7A

(S)

b5
b6
b7C

~~SECRET~~

~~SECRET~~

b5
b6
b7C
b7A

b5
b7A

(S)

(S)

(S)
(S)

b1
b5
b7A

~~SECRET~~

intelligence needs. [redacted] (S)

b1 [redacted] (S)
b5
b7A [redacted]

[redacted]

b5 [redacted]
b6
b7C

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

b5 [redacted]

101 d. OGC. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

[redacted]

b5
b6
b7C

100 e. CTD (in coordination with OGC). Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.

b1
b5
b6
b7C

[redacted] (S)

103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

b1
b5
b7A

[redacted] (S)

~~SECRET~~

(S)

b1
b5
b6
b7C
b7A

~~SECRET~~

coordination, law enforcement agents and prosecutors learned from intelligence officers that an April 2003 telephone conversation between Dumeisi and a co-conspirator corroborated evidence that Dumeisi was acting as an agent of the Iraqi government, providing a compelling piece of evidence at Dumeisi's trial.

b. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

b5

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

b5

93. Section 220 of the USA-Patriot Act, "Nationwide Service of Search Warrants for Electronic Evidence" allows for the execution of a search warrant seeking electronic data anywhere in the country. This question pertains to the implementation of this provision since its passage.

a. In how many cases has this authority been used?

Response:

While the FBI does not require or maintain centralized statistics on the use of search warrants, Field Offices indicate that they have routinely relied on this

provision (codified at 18 U.S.C. 2703(a)) and can safely estimate that, nationwide, this search authority has been used at least 100 times since its passage.

In section 220 of the USA PATRIOT Act, Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The ability to obtain this information with greater efficiency has proven invaluable in numerous cases, including: several terrorism investigations (such as the Virginia Jihad case described above and a complex terrorism financing case in which it was used to obtain a subject's e-mail related to a 7/4/02 shooting at Los Angeles International Airport); child pornography cases in which it is used to obtain information from ISPs regarding those trading sexually exploitive images of children; investigations of "carders" (those who use and trade stolen credit card information); and numerous investigations into Internet sales of counterfeit products, which have led to several indictments and the seizure of bank and financial accounts.

Child pornography cases highlight the benefit of Section 220, because the ability to obtain a search warrant in the jurisdiction of a child pornography investigation rather than in the jurisdiction of the ISP is critical to the success of a complex, multi-jurisdictional child pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country so they could obtain warrants in those jurisdictions, or travel hundreds or thousands of miles to present warrant applications to local magistrate judges. Without Section 220, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

The following case, included in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work," provides an additional example of the benefits afforded by Section 220. A man, armed with a sawed-off shotgun, abducted his estranged wife and sexually assaulted her. Then, after releasing his wife, he fled West Virginia in a stolen car to avoid capture. While in flight, he contacted cooperating individuals by e- mail using an Internet service provider (ISP) located in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, including the California ISP. Within a day of the order's issuance, the ISP released information revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and noticed a carnival set up next to the public library. Because they were aware that the fugitive had previously worked as a carnival

worker, the Deputy Marshals went to the carnival and discovered the stolen car, arresting the fugitive as he approached the car. He later pled guilty in state court and was sentenced to imprisonment for 30 years. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account, made possible by section 220 of the USA PATRIOT Act, was crucial to his capture.

Section 220 has also made the process of obtaining a warrant for ISP information much more efficient. Before the USA PATRIOT Act, judicial districts that are home to large ISPs were inundated with search warrant requests for electronic evidence. For example, the U.S. Attorney's Office in Alexandria, Virginia, was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for the records of an ISP located there. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all the details of another district's investigation in order to present an affidavit to the court in support of the search warrant application. Because of section 220, however, these attorneys and Agents can now spend their time on local cases and investigations rather than on learning the details of unrelated investigations being worked through distant offices. Given the short time for which ISPs typically retain records, this provision has enabled the FBI to obtain critical information that may otherwise have been lost or destroyed in the ordinary course of the ISP's business. Section 220 also results in a more efficient use of judicial resources by allowing the judge with jurisdiction over the offense to issue the warrant and retain oversight over the search.

b. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

b5

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

The FBI has interviewed Padilla and other enemy combatants. FBI Agents conducting interviews of enemy combatants adhere to the FBI policy governing interviews of persons in the U.S., with the one exception that enemy combatants are not advised of Miranda rights prior to the interrogation.

b. How many individuals have been arrested or detained pursuant to this authority?

c. How many United States citizens have been arrested or detained pursuant to this authority?

d. How many United States persons, as defined in Executive Order 12333, Section 3.4(i), and excepting United States citizens, have been arrested or detained pursuant to this authority?

Response to b through d:

Information concerning the designation and detention of enemy combatants is not maintained by the FBI.

e. What rules, procedures or practices govern the conditions of confinement and the methods of interrogation used in cases where an individual has been arrested or detained pursuant to this authority?

Response:

Rules, procedures, and practices concerning the conditions of confinement and methods of interrogation of enemy combatants by DOD are not maintained by the FBI. When FBI Agents interview enemy combatants or detainees, standard FBI interview policies and practices apply.

82. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107-56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeapor[dize] an investigation or unduly [delay] a trial" been used? Please describe the circumstances in each of these cases?

Response:

b5

83. Sections 201 and 202 of the USA-Patriot Act added a number of offenses to the "predicate offense list" applicable to criminal wiretaps pursuant to Chapter 119 of Title 18. The following question pertains to the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. In how many cases . . . have the newly-added predicate offenses been used to support an application for a criminal wiretap under the authority of Chapter 119 of Title 18?

Response:

The FBI applied for Title 18 wiretap orders in eight investigations into international terrorism since passage of the USA PATRIOT Act. In only one of those investigations was a newly added terrorism offense used as the sole predicate offense; traditional criminal offenses were used as the predicates for the remaining seven. It cannot be determined, however, whether probable cause as to one or more of the new terrorism predicate offenses was also established, but simply not listed, in those seven cases.

b. In how many such cases has the newly-added predicate offense been the only predicate offense asserted as the basis for the warrant, i.e., where a warrant could not have been lawfully issued but for the passage of the additional criminal predicates?

Response:

In the one case referred to above, the terrorism predicate was the only one asserted. It is not known, however, whether there was probable cause to believe the subjects were engaging in other predicate offenses which were simply not listed, or whether there was probable cause only with respect to the terrorism offense.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Sections 201 or 202 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

b5

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute, including the addition of predicate crimes, which the Congress should consider?

Response:

Sections 201 and 202 of the USA PATRIOT Act are currently scheduled to expire at the end of 2005. The FBI strongly supports making these important statutory provisions permanent. In addition, the FBI would ask Congress to consider amending 18 U.S.C. 2516 to allow for the use of existing electronic surveillance authorities in investigating the full-range of terrorism related crimes. In particular, Congress should consider adding the following predicate offenses to those currently listed in 18 U.S.C. 2516(1): 1) 18 U.S.C. 37 (relating to violence at international airports); 2) 18 U.S.C. 930(c) (relating to an attack on a federal facility with a firearm); 3) 18 U.S.C. 956 (conspiracy to harm persons or property overseas); 4) 18 U.S.C. 1993 (relating to mass transportation systems); 5) an offense involved in or related to domestic or international terrorism as defined in 18 U.S.C. 2331; 6) an offense listed in 18 U.S.C. 2332b(g)(5)(B); and 7) 18 U.S.C. 2332d.

While the few statistics listed in response to questions 83 a and b, above, may be understood to indicate limited use of this new authority and limited value of these new USA PATRIOT Act sections, this would not be correct. In most international terrorism investigations since October 2001, electronic surveillance

has been successfully pursued under FISA authority and, therefore, the criminal terrorism predicates under Title 18 were not necessary. Nevertheless, in future investigations in which probable cause regarding connection to a foreign power cannot be as easily established (and thus FISA surveillance is not an option), these new USA PATRIOT Act provisions will permit the use of a federal wiretap in response to significant terrorist threats. The flexibility to use either foreign intelligence collection tools or criminal evidence gathering processes, and to share the results, is an important feature of the USA PATRIOT Act in the war against terrorism.

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same [A]ct makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response:

On 9/23/02, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the USA PATRIOT Act. Those guidelines, and the FBI's instructions to the field with respect to those guidelines, follow.

b. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the USIC through any means appropriate to the circumstances, including Intelligence Information Reports (IIRs), Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(b) material?

Response:

The FBI disseminates intelligence information via the IIR, which is an electronic communication format widely accepted in the USIC as the standard intelligence dissemination vehicle. IIRs consist of raw intelligence (intelligence which has not been finally evaluated) and associated clarifying information that puts the raw intelligence into context. IIRs are drafted and prepared by the FBI's cadre of Intelligence Analysts/Reports Officers. Before FBI intelligence is disseminated, it is analyzed and sanitized to protect intelligence sources and methods and, if applicable, United States persons and entities that may be compromised or negatively impacted if left unprotected. FBI Program Managers and Intelligence Analysts concurrently identify intelligence that is consistent with USIC intelligence requirements and interests.

(1) If so, how many such reports have been issued?

Response:

Although CTD is not the only FBI producer of IIRs, that Division reports that, during the period from August 2002 (when statistical data was first collected) through August 2004, CTD has disseminated approximately 3,860 IIRs, 240 of

which have contained FISA-derived intelligence. The remaining IIRs have been derived from various sources and methods which may or may not include Title III information.

The FBI does not track or maintain a central database with respect to the number of IIRs containing 203(b) material, if any.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Determinations to disseminate electronic, wire, and oral intercept information are made with input from Operational Program Managers, Intelligence Analysts, the National Security Law Branch, and, when appropriate, DOJ. This evaluation considers the value of the information not only to the USIC but also, depending on the proposed use, context, and nature of any threat-related information, to federal, state, and local law enforcement entities and, when authorized by DOJ, to foreign intelligence services and foreign law enforcement agencies.

The quality and value of IIRs are evaluated through several means. On each IIR, the Reports Officer provides information by which the customers can contact the Reports Officer directly. The quality and relevance of the reporting is also reflected by the submission of additional collection requirements; USIC members often forward formal Requests for Information (RFIs) with respect to information that has been protected (not provided) in the IIR, such as U.S. Person information. Such RFIs provide an excellent indication of USIC interest in FBI reporting. In addition, USIC members often provide feedback with respect to specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. The FBI's OI also often receives evaluations of FBI reporting, and is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

c. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response:

The FBI shares foreign intelligence information, as defined in Section 203(d)(2), with the USIC through several conduits. Dissemination can be through direct classified and unclassified IIRs, Intelligence Assessments, Intelligence Bulletins, Teletype Memoranda, or USIC web sites on classified networks. The FBI also shares intelligence information through the FBI's Joint Terrorism Task Forces (JTTFs), which include members of the USIC and operate in 84 locations across the United States. Unclassified but "law enforcement sensitive" intelligence information is also disseminated to federal, state, and local law enforcement intelligence components through Law Enforcement Online (LEO), a computer network which provides finished intelligence products, assessments, and bulletins on significant developments and trends.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the USIC through any appropriate means, including IIRs, Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(1) If so, how many such reports have been issued?

Response:

While the FBI does not track or maintain a central database with respect to the number of IIRs containing 203(d) material, if any, the July 2004 DOJ "Report From the Field: The USA PATRIOT Act at Work" indicates that DOJ has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, to track terrorists' funding sources, and to identify terrorist operatives overseas.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

There are various means by which IIRs are evaluated. Members of the USIC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify the means by which customers can contact them directly. IC members assess the quality and relevance of the reporting, and submit additional collection requirements when appropriate. Often, IC members forward formal Requests for Information (RFIs), which can provide an excellent indication of IC interest in FBI reporting. The FBI's OI also receives evaluations of FBI reporting. The OI is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

d. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response:

b5

e. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

b5

f. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

b5

b5

[redacted]

85. Section[ ] 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains [to] the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. How often has this authority been used, and with what success?

Response:

b5

[redacted]

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response:

FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. The FBI shares many forms of foreign intelligence with other members of the USIC through direct classified and unclassified disseminations, through web sites on classified USIC networks, through its participation in Joint Terrorism Task Forces (JTTFs), and through its collaboration in activities abroad.

FBI intelligence products shared with the USIC include IIRs, Intelligence Assessments, and Intelligence Bulletins. The FBI also disseminates intelligence information through LEO, a virtual private network that reaches federal, state, and local law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes available to all users finished FBI intelligence products, including intelligence assessments resulting from the analysis of criminal, cyber, and terrorism intelligence, finished intelligence concerning significant developments or trends, and IIRs that are available at the SBU level. In addition, the FBI

recently posted the requirements document on LEO, providing to state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response:

In the past two years, CTD's Terrorism Reports and Requirements Section has disseminated 76 IIRS containing information derived from FISA-authorized surveillance and/or searches. (Statistics are not maintained in a way that would enable us to advise whether any of the FISA-derived information in the reports was obtained using roving wiretap authority.) Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 IIRs containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

The OI promulgated the FBI's Intelligence Information Report Handbook on 7/9/04. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The OI is also working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with law enforcement and USIC partners.

In addition, the FBI's Inspection Division has established criteria for assessing: the value of human source reporting; access to and the responsiveness of local FBI field offices; and FBI program and national intelligence requirements. The OI is developing guidelines according to which it will use these same criteria as a means of assessing the value of raw intelligence. Initial discussions on this issue have been held with the CI, CT, Criminal, and Cyber Divisions, and the results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being

adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response:

No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept the conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, for surveillance of all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the FISA Court issue, along with the primary order, a "generic" secondary order with respect to a specifically identified FISA target that the FBI can serve in the future on a currently unknown cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear, in a detailed affidavit, to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. While the roving order carries the additional requirement of a judge's approval to monitor more than one telephone, it permits government agents to continue to monitor the target, even if the target changes to a different cellular telephone, rather than first going through the lengthy application process to monitor that new phone. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the FISA Court for a new secondary order. The FBI views this as a vital tool to counter targets who change cell phone providers or other communication channels as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response:

The FBI has filed no such briefs on this subject.

d. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act? If so, please describe the nature and disposition of such a complaint.

Response:

b5

e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

Response:

b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate?

Response:

None of which the FBI is aware.

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

b5

[redacted]

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

None at this time.

87. Section 209 of the USA-Patriot Act clarified the law with regarding the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. How many such search warrants have been issued since passage of this act?

Response:

The FBI does not collect or maintain statistics concerning the types of search warrants issued in FBI investigations, including those seeking access to voice mail. Because federal search warrants are requested by U.S. Attorneys' Offices and issued by U.S. District Courts, these statistics may be maintained by one or both of those offices.

b. In such cases, have there been any instances in which a wiretap, as opposed to a search[ ] warrant[,] would not have been supported by the facts asserted in support of the search warrant.

Response:

This information is unavailable, as indicated above. It is clear, however, that the support needed for a federal wiretap is considerably greater than that required for a search warrant.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

A private citizen who has lodged numerous complaints against the FBI, all of which have been determined to be unfounded pursuant to appropriate inquiry, complained that she was a former FBI employee whose home, vehicles, telephone, and internet had been subject to "aggressive surveillance" since August 2000. FBI investigation revealed that the complainant was, in fact, not a former FBI employee and that the FBI had conducted no surveillance of her for any reason. Based on these findings, this matter was closed by the FBI in July 2003. The FBI has construed this as a complaint with respect to both Section 209 and 217 of the USA PATRIOT Act.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI is not aware of any substantive changes to this provision warranting Congressional consideration. Section 209 is, however, currently scheduled to expire at the end of 2005, and the FBI strongly supports making this provision permanent. Section 209 allows investigators to use court-ordered search warrants to obtain voice-mail messages held by a third party provider when supported by probable cause. Previously, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. 2703, allowed law enforcement authorities to use search warrants to gain access to stored electronic communications such as e-mail, but not stored wire communications such as voice-mail. Instead, the wiretap statute, 18 U.S.C. 2110(1), governed access to stored wire communications, requiring law enforcement officers to use wiretap orders to gain access to unopened voice-mail. This resulted in voice-mail messages being treated differently than e-mail messages. Voice-mail messages are also treated differently than answering machine messages inside a home, access to which requires a search warrant, because answering machine messages are not regulated under the wiretap statute. Section 209 of the USA PATRIOT Act eliminates the disparate treatment of

similar information. If this section is sunsetted, voice-mail messages will again be treated in a different manner than answering machine messages and stored e-mail information beginning in 2006.

88. Section 212 of the USA-Patriot Act permits communications service providers to provide customer records or the content of customer communications to the FBI in an emergency situation. This question pertains to application of this provision since its passage, and to all instances, not only to terrorism investigations.

a. In how many cases has this provision been used? Please provide a short description of each such case to the Committee.

Response:

Service providers have voluntarily provided information on at least 141 occasions under this provision. Such disclosures have often included both e-mail content and associated records. Several of these disclosures have directly supported terrorism cases under the emergency of a possible pending attack. For example, this provision has been used to obtain access to e-mail accounts used by terrorist groups to discuss various terrorist attacks. It has also been used to respond quickly to bomb and death threats, as well as in an investigation into a threat to a high ranking foreign official. This provision has additionally been used to locate kidnaping victims and to protect children in child exploitation cases. In one kidnaping case involving the abduction of a 14-year-old girl, reliance on this provision allowed the FBI to quickly locate and rescue the child and to identify and arrest the perpetrator. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours.

Because many international service providers are located within the United States (such as Hotmail and AOL), Legal Attachés have used this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss of life or serious injury.

Additional examples are provided in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work."

b. In any such case have there been any cases in which, except for the time constraints imposed by the emergency situation, a conventional wiretap or search warrant,

would not have been supported by the facts available to the Government at the time of the emergency request? If so, please describe such situations.

Response:

We are aware of no such circumstances. However, it is important to recognize that the information that may be disclosed under this emergency authority is limited to the contents of communications that are in electronic storage and records associated with customers or subscribers. Given this limitation, a conventional wiretap would generally not apply, and a search warrant would be required only for the contents of communications that are held for less than 180 days. Emergency authority is appropriate for the disclosure of information held by a third party and, to the extent the information is constitutionally protected, disclosure of the information under exigent circumstances is entirely consistent with the emergency exception to the warrant requirement of the Fourth Amendment.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

b5

[redacted]

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

There is currently a discrepancy between the emergency provisions applicable to contents and records that appears illogical and unjustified. Currently a provider is arguably required under 18 U.S.C. 2702(c)(4) to meet a higher burden for disclosing a record or other subscriber information than is required by § 2702(b)(7) for divulging the contents of a communication in electronic storage. Moreover, the entities to whom a provider may disclose are significantly more restricted for records than for content. The language in (b)(7) was enacted by Pub. L. 107-296 as part of the Homeland Security Act of 2002, with the objective that

all entities with responsibility for ensuring our domestic security would have access to this information in an emergency. It does not appear that the discrepancies between the disclosure of content and records are supported by differing privacy interests inherent in the respective information or by other factors. Accordingly, reconciling these provisions would be appropriate.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. In how many cases has this authority been used?

(i) How many of such cases were terrorism-related?

Response to a and a(i):

The FBI does not maintain this information. It is, instead, maintained by DOJ's OIPR, to whom the FBI defers for response.

b. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response:

The FBI does not track the number of pen registers that evolve into full FISA's.

c. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.

Response:

The FBI has not developed any such regulations or directives, nor is it aware that the USIC or DOJ have issued guidance defining "non-content communications" in relation to the use of FISA pen register/trap and trace authorities.

d. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

See response to Question 85b, above.

(i) If so, how many such reports have been issued?

Response:

See response to Question 85b(i), above.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

See response to Question 85b(ii), above.

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response to a and b:

[redacted] b5

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be premised solely upon the exercise of constitutionally protected activities.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA). At the FBI field level, such requests must be approved by the Supervisory Special Agent (SSA), the SAC or appropriate Assistant SAC, and the Chief Division Counsel. At the FBIHQ level, the request must be approved by an attorney in the National Security Law Branch, and signed by one of the several designated high-ranking FBI officials to whom certification authority has been delegated. Thereafter, the request is submitted to DOJ's OIPR, and must be approved by OIPR before it is presented to the FISA Court. When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

[redacted] b5

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence activities conducted by the USIC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

None of the information contained in the 3,860 terrorism-related IIRs disseminated between August 2002 and August 2004 was acquired pursuant to section 215 of the USA PATRIOT Act.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Although the FBI has procedures to evaluate the quality of intelligence reports, no reports have been disseminated which contained information acquired pursuant to section 215 of the USA PATRIOT Act.

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

b5

[redacted]

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

91. Section 217 of the USA-Patriot Act authorizes, without court order, the interception of communications to and from a trespasser with a protected computer. This question pertains to the implementation of this provision since its passage.

a. How many times has the authority under this section been used, and with what success? Please provide descriptions of the circumstances where it has been used.

Response:

While the FBI does not maintain statistics on the frequency with which the trespasser authority has been used, we can provide examples of some such cases.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). This group used chat rooms and fraudulent web sites, creating false identities to obtain e-mail accounts and then transmitting their communications through a computer that had been "hacked" and set up to operate as their proxy server. A proxy server changes an Internet user's original Internet protocol (IP) address to that of the proxy server so that only the proxy server knows the true point of origin. The owner of the hacked computer was not aware that it was being used as a proxy server, and considered all individuals using the system as a proxy server to be trespassers. The owner provided the FBI with consent to monitor the communication ports solely used by the trespassers, and this monitoring led to the subject's true identity. The subject was indicted in September 2003. Without this authority to monitor, the real identities of the trespassers could easily have remained anonymous.

In another example, a former employee was suspected of illegally accessing a company's e-mail system to gain inside information regarding company concepts

and client information, as well as privileged information regarding legal proceedings between the company and the former employee. The computer intruder used a variety of means to access the system, including wireless modems in laptops and hand-held Blackberry devices, making it more difficult to identify the intruder and to link the computer intrusions to the former employee. The victim company authorized the FBI to monitor the intruder's communications with and through its computer systems.

In another case, a computer-intruder obtained control of a school's network and reconfigured it to establish additional IP addresses that were separate and distinct from those used by the school. This allowed hackers, and others using the Internet who did not want to be located, to jump through the school's system before committing their illegal acts. Monitoring accomplished pursuant to the school's consent resulted in the FBI's identification of over 200,000 different IP addresses using the school system as a proxy to further illegal activity such as fraud, computer intrusions, and spamming.

As these cases make clear, this authority is critical not only to the FBI's ability to identify criminals who engage in computer intrusions but also its ability to identify and investigate additional criminal activities conducted through victims' computers.

b. Section 217(2)(I) requires authorization by the owner of the computer before the section can be applied. Can this authorization be withdrawn or limited by the owner of the computer? If so, how and in what circumstances?

Response:

Yes. As with any form of consent, which must be freely and voluntarily given to be valid, the consenting party has the right to terminate the consent at any time. The FBI encourages the use of a written consent form containing an express acknowledgment by the consenting owner or operator that states: "I understand my right to refuse authorization for interception and have accordingly given this authorization freely and voluntarily."

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

See response to Question 87c, above.

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

Response:

As indicated in the July 2004 DOJ publication entitled, "Report from the Field: The USA PATRIOT Act at Work," the removal of the "wall" played a crucial role in the Department's successful dismantling of a Portland, Oregon, terror cell, popularly known as the "Portland Seven." Members of this terror cell had attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned through an undercover informant that, before the plan to go to Afghanistan was formulated, at least one member of the cell, Jeffrey Battle, had contemplated attacking Jewish schools or synagogues, and had even been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they suspected that a number of others were involved in the Afghanistan conspiracy. While several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them. Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack; if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would undoubtedly have scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets, and could keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely, but instead to continue to gather evidence on the other cell members. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were

dismissed after he was killed in Pakistan by Pakistani troops on 10/3/03.

b5

DOJ shared information pursuant to sections 218 and 504 before indicting Sami al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist organizations, responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that al-Arian served as the secretary of the PIJ's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ. Sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against al-Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to prosecutors' ability to build their case and pursue the proper charges.

b5

Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the so-called "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, some of whom trained for jihad in Northern Virginia by participating in paintball and paramilitary training or traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against several individuals. Nine of these defendants have received sentences ranging from four years to life imprisonment (six were pursuant to guilty pleas and three were contrary to their pleas; charges have included conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban).

Information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was also pivotal in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. Based upon information obtained

through an FBI undercover investigation, the complaint alleges that Al-Moayad had boasted that he had personally handed Usama Bin Laden $20 million from his terrorist fund-raising network and that Al-Moayad and Zayed had flown from Yemen to Frankfurt, Germany, in 2003 with the intent to obtain $2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would be used to support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Al-Moayad and Zayed were extradited to the United States from Germany in November 2003 and are currently awaiting trial.

Sections 218 and 504 were also used to gain access to intelligence that facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden, and used his charities both to obtain funds for terrorist organizations from unsuspecting Americans and to serve as a channel for people to contribute money knowingly to such groups. Arnaout pled guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the San Diego prosecution of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they had conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they had conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

Sections 218 and 504 were also critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq and of two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA shared information with law enforcement agents and prosecutors investigating Dumeisi. Through this

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 7
Page 114 ~ Duplicate
Page 115 ~ Duplicate
Page 116 ~ Duplicate
Page 117 ~ Duplicate
Page 118 ~ Duplicate
Page 119 ~ Duplicate
Page 120 ~ Duplicate

DATE: 12-05-2005
FBI INFO.
CLASSIFIED BY 65179 DMH/LP/DFW
REASON: 1.4 ((C) 05-CV-0845)
DECLASSIFY ON: 12-05-2030

b6
b7C

From: [redacted] CTD) (FBI)
Sent: Thursday, March 31, 2005 1:01 PM
To: HEIMBACH, MICHAEL J. (CTD) (FBI); [redacted] (CTD) (FBI); HULON, WILLIE T. (CTD) (FBI)
Cc: HQ-DIV13-ITOS I
Subject: Patriot Act Roving Authority - ITOS1 response

SECRET
RECORD n/a

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Hello,

(S) [redacted]

b1
b2
b7E
b5

Example:

(U) [redacted]

b2
b7D
b7E

[redacted]

CTD/ITOS-1
FBIHQ [redacted]
desk: [redacted]
page [redacted]

b2
b6
b7C

-----Original Message-----
From: HULON, WILLIE T. (CTD) (FBI)
Sent: Wednesday, March 30, 2005 9:24 PM
To: Caproni, Valerie E. (OGC) (FBI); VANNUYS, THOMAS J. (CTD) (FBI); HEIMBACH, MICHAEL J. (CTD) (FBI)
Subject: RE: Help

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Tom/Mike,
Please provide info re this by noon, Thursday.
Thanks
Willie T.

SECRET

-----Original Message-----
From: Caproni, Valerie E. (OGC) (FBI)

b6
b7C

Sent: Wednesday, March 30, 2005 6:51 PM
To: BALD, GARY M. (DO) (FBI); HULON, WILLIE T. (CTD) (FBI); SZADY, DAVID (CD) (FBI); PISTOLE, JOHN S. (DO) (FBI); FEDARCYK, MICHAEL R. (DO) (FBI)
Cc: KALISCH, ELENI P. (OCA) (FBI)
Subject: Help

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S)

In the draft of testimony for the AG, they are

b1
b2
b7E
b5

SENSITIVE BUT UNCLASSIFIED

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

SECRET

b6
b7C

~~SECRET~~

From: [redacted] (CTD) (FBI)
Sent: Thursday, March 17, 2005 4:51 PM
To: HEIMBACH, MICHAEL J. (CTD) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: RE: Patriot Act & library records

b6
b7C
b6
b7C

DATE: 12-05-2005
CLASSIFIED BY 65179 DMH/LP/DFW
REASON: 1.4 ((C) ,05-CV-0845)
DECLASSIFY ON: 12-05-2030

~~SECRET~~
RECORD [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

The answer is: b2

- Requests pursuant to the Patriot Act business records/library records provision would be executed via NSLs
- [redacted] (S)

b1
b2
b7E
b5

Ta-da. Thanks [redacted]

b6
b7C

[redacted]
CTD/ITOS-1
FBIHQ [redacted]
desk [redacted]
pager [redacted]

b2
b6
b7C

-----Original Message-----
From: HEIMBACH, MICHAEL J. (CTD) (FBI)
Sent: Thursday, March 17, 2005 11:56 AM
To: [redacted] (CTD) (FBI)
Subject: FW: Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

See if this is something we track and/or can retrieve. Thanks Mike

Section Chief Michael J. Heimbach
CTD/ITOS I
Office # 571-280-5267
Pager # [redacted]
Cell # [redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Thursday, March 17, 2005 11:48 AM
To: [redacted] CTD) (FBI); HEIMBACH, MICHAEL J. (CTD) (FBI); VANNUYS, THOMAS J. (CTD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI)
Subject: FW: Patriot Act

~~SECRET~~

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

Please look at the request below from EAD Bald, which came to us through AD Hulon. Is this somehow picked up on the scorecard you generate for the visiting SACs?

Mike & Tom,

Is this something that either of the ITOS units monitor?

Thank You, b6

[redacted] b7C

-----Original Message-----
From: HULON, WILLIE T. (CTD) (FBI) b6
Sent: Thursday, March 17, 2005 11:27 AM b7C
To: [redacted] (CTD) (FBI)
Cc: BALD, GARY M. (DO) (FBI); [redacted] (CTD) (FBI); [redacted] (CTD) (FBI); [redacted] (DO) (FBI)
Subject: FW: Patriot Act

UNCLASSIFIED
NON-RECORD b6

[redacted] b7C

Please determine if there is a mechanism for determining the instances when the use of the Patriot Act 215 has been employed in CT matters. If so, please provide the stats.
Thanks
Willie T.

-----Original Message-----
From: BALD, GARY M. (DO) (FBI)
Sent: Thursday, March 17, 2005 8:32 AM
To: REIGEL, LOUIS M. (CyD) (FBI); HULON, WILLIE T. (CTD) (FBI); Caproni, Valerie E. (OGC) (FBI)
Cc: PISTOLE, JOHN S. (DO) (FBI); STEELE, CHARLES M (DO)(FBI)
Subject: Patriot Act

UNCLASSIFIED
NON-RECORD

Lou - This morning, the Director asked Dave Thomas, CyD for details concerning the number of times library computers have been used to launch cyber attacks. In particular, he wants this information in anticipation of questions that will arise during consideration of the sunset clauses in the Patriot Act. Would you please follow-up with Dave on this request, and include me in the response, which should be sent to the Director through Charlie Steele.

In addition, I believe it would be helpful to reliably determine [redacted] If the information is available in either CTD or OGC, would you, Willie and Val, please also forward this to Charlie (cc to me). b2 b7E

Val - If we do not currently require [redacted] b5

[redacted] Thx. Gary b6 b7C

SECRET

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

SECRET

b6

b7C

~~SECRET~~

From: [redacted] (CTD) (FBI)
Sent: Thursday, March 17, 2005 12:43 PM b6
To: HEIMBACH, MICHAEL J. (CTD) (FBI) b7C
Cc: [redacted] (OGC) (FBI)
Subject: RE: Patriot Act

UNCLASSIFIED
NON-RECORD

(S)

[redacted] There is no tracking method for that specifically in ITOS1, [redacted] b1 b5

I spoke to NSLB, and they are going to double-check to confirm that [redacted] b2
[redacted] I spoke to [redacted] who noted [redacted] I'll get back to you as soon as I get confirmation of the above. b7E

[redacted] b6 b7C

CTD/ITOS-1
FBIHQ [redacted] b2
desk: [redacted] b6
pager: [redacted] b7C

-----Original Message-----
From: HEIMBACH, MICHAEL J. (CTD) (FBI)
Sent: Thursday, March 17, 2005 11:56 AM b6
To: [redacted] (CTD) (FBI) b7C
Subject: FW: Patriot Act

UNCLASSIFIED
NON-RECORD

See if this is something we track and/or can retrieve. Thanks Mike

Section Chief Michael J. Heimbach
CTD/ITOS I
Office # 571-280-5267
Pager # [redacted]
Cell # [redacted] b2
[redacted] b6
-----Original Message-----
From: [redacted] (CTD) (FBI) b7C
Sent: Thursday, March 17, 2005 11:48 AM
To: [redacted] (CTD) (FBI); HEIMBACH, MICHAEL J. (CTD) (FBI); VANNUYS, THOMAS J. (CTD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI)
Subject: FW: Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b6

~~SECRET~~ b7C

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 2
Page 8 ~ Duplicate
Page 9 ~ Duplicate

[redacted]OGC) (FBI)

From: [redacted] b6
Sent: Monday, October 20, 2003 9:39 AM b7C
To: [redacted]
Subject: Fwd: Re: Business Records

Forwarded Mail received from: [redacted]

-----Original Message-----
Date: 10/16/2003 03:48 pm -0400 (Thursday)
From: [redacted]
To: [redacted] b6 b7C
CC: BOWMAN, MARION, Rowan, J
Subject: Re: Business Records

Thanks for teeing up this issue - again. Rather than dragging their collective feet or setting up hurdles - OIPR should be embarrassed that the FBI has used this valuable tool to fight terrorism - exactly ZERO times. The inability of FBI investigators to use this seemingly effective tool has had a direct and clearly adverse impact on our terrorism cases. Quite frankly, Agents have spent the last 2 years screwing around with weak NSLs or using made up "voluntary" NSLs literally begging people to give us information in our terrorism cases (try to get info from [redacted]). The fact that this new FISA tool has languish for two years - with no likely usage in the future - is nuts. While radical militant librarians kick us around - true terrorists benefit from OIPR's failure to let us use the tools given to us. THIS SHOULD BE AN OIPR PRIORITY!!! b2 b7E

In any event - the efforts of NSLB to get this on track are greatly appreciated. (PS - don't forget OIPR's [redacted] the same story)

[redacted]
WFO Office of Division Counsel [redacted] b6 b7C

Privileged and ~~Confidential~~ b2

>>> [redacted] 10/16 2:56 PM >>>
Not surprisingly, we (I should say, Pat Rowan) presented OIPR with a finalized application and proposed order for business records, signed by Valerie, and they were all up in arms because we had not coordinated in advance and had not used the form they had and because we are not authorized to appear before the court and they don't have enough information about the target and . . . I guess, mainly, they were upset because we wanted to accomplish something without their interference. After Pat went through all their grievances and asked whether they would file something that used their form and met their informational needs, [redacted] said that it would depend on OIPR priorities. Which means, I guess, that we get business records after the last of the initiations sitting on their desks has been filed.

Anyway, does anyone have or has anyone heard of a business records form that OIPR has already produced. [redacted] said that [redacted] would have it but then conceded that he probably would not. Also, per FISC Rule 9, we are told that we cannot file something with the court or cannot appear in Court unless we are on some authorized list. Does anyone have a copy of the FISC rules?

I guess it was too good to be true, that we would actually be able to file something with the FISA Court with our names on it and without it being held up by OIPR.

More on this saga to come .. . ..

[redacted] b6 b7C

b6
b7C

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Friday, May 21, 2004 12:04 PM
To: [redacted]

b6
b7C

Subject: MIRACLES

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED
NON-RECORD

We got out first business record order signed today! It only took two and a half years.

[redacted]

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 06/6/2003

To: All Divisions Attn: ADIC, AD, DAD, SAC, CDC

From: Office of the General Counsel
National Security Law Unit
Contact: [redacted]

Approved By: Mueller Robert S III

Drafted By: [redacted]

Case ID #: 66F-HQ-A1247863

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-27-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

Title: FISA BUSINESS RECORD APPLICATIONS
DELEGATION OF AUTHORITY

Synopsis: Delegates signature authority for Applications for Business Records to FBIHQ officials under 50 U.S.C. § 1861.

Details: The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C § 1861, provides for access to certain business records for foreign intelligence (FI) and international terrorism (IT)investigations through issuance of an order from the FISA Court (FISC). Section 1861(a)(1) authorizes the "Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge)" to make an application for the order.

Thus, as permitted by 50 U.S.C. § 1861(a)(1), I hereby designate certification signature authority for applications for FISA business records to the following FBI Officials:

1. The Deputy Director;

2. The Executive Assistant Director for Counterterrorism/Counterintelligence;

3. The Assistant Directors and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; and

4. The General Counsel; the Senior Counsel for National Security Affairs; and the Deputy General Counsel for National Security Affairs.

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ, 06/6/2003

The National Security Law Unit is hereby authorized to prepare business record applications and will issue guidance on the application process.

LEAD:

Set Lead 1: (adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in CI, IT, and Cyber operations and to other personnel as appropriate.

[redacted] (OGC) (FBI)

From: [redacted]
Sent: Wednesday, February 25, 2004 10:17 AM
To: [redacted]
b6
b7C
Subject: FW: Simulateous use of criminal and FISA instruments

-----Original Message-----
From: Caproni, Valerie E.
Sent: Tuesday, February 24, 2004 5:29 PM
To: Curran, John F; BOWMAN, MARION E.; [redacted]
Cc: [redacted] MUELLER, ROBERT S. III; WAINSTEIN, KENNETH L.
Subject: Simulateous use of criminal and FISA instruments

b6
b7C

Effective immediately DOJ is no longer objecting to the simultaneous use of criminal and FISA tools. Please pass this along to all the NSLU attorneys promptly. [redacted]

b5

VC

(Rev. 08-28-2000)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 03/07/2003

To: Counterterrorism Attn: SSA [redacted]
SSA [redacted]
IOS [redacted]

b2
b6
b7C

From: Office of the General Counsel
National Security Law Unit (NSLU)/Room [redacted]
Contact: [redacted]

DECLASSIFIED BY 65179 DMH/CLS
ON 09-27-2005

Approved By: Bowman M. E.

Drafted By: [redacted]

Case ID #: (U) 66F-HQ-A1247863 (None)

b6

Title: (U) [redacted]

b7C

Synopsis: ~~(S)~~ (U) This communication conveys NSLU authorization to declassify certain FISA-derived documents for use by the U.S. Attorney's Office for [redacted] in criminal proceedings of [redacted]

~~Derived From : Multiple Sources~~ (U)
~~Declassify On: X1~~

Reference: ~~(S)~~ (U) 199N-SE-85481 (Pending)

Details: ~~(S)~~ (U) Pursuant to a request from the International Terrorism Operations Section I, CONUS 2, Team 7, NSLU reviewed FISA-derived material contained in a memorandum dated 02/12/2003 from FBI Assistant Director Larry Mefford to [redacted] Counsel, Office of Intelligence Policy and Review, Department of Justice. The memorandum was seeking authorization from the Attorney General to use information obtained or derived from the electronic surveillance and physical searches of [redacted] in any and all phases of criminal prosecution. NSLU reviewed the documents and determined that the cuts contained in the 02/12/2003 memorandum could be declassified. NSLU received confirmation from CONUS 2 that none of the information reviewed came from [redacted] surveillance of [redacted]

b6
b7C

b2
b7E

~~SECRET~~

To: Counterterrorism From: Office of the General Counsel
Re: (U) 66F-HQ-A1247863, 03/07/2003

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, D.C.

(U) Authorization provided by NSLU for the declassification of certain documents associated with the criminal prosecution of [redacted].

CC: 1 - Mr. Bowman
1 - [redacted]

b6
b7C

♦♦

[redacted] OGC) (FBI)

From: [redacted]
Sent: Thursday, October 09, 2003 1:46 PM
To: [redacted]
b6
b7C

Cc:
Subject: FW [redacted] FISA Issue

b2
b7E

Forwarded FYI is WFO's response to a complaint that [redacted] was processing FISA warrant searches in a timely or complete manner. Should you become aware of a similar complaint in the future I recommend that you contact [redacted] and let him check it out. He was very helpful and timely in his response.

b6
b7C

[redacted]

-----Original Message-----
From: [redacted]
Sent: Thursday, October 09, 2003 1:27 PM
To: [redacted]
Cc: [redacted]; BOWMAN, MARION E.; [redacted]
Subject: [redacted] FISA Issue

b2
b7E

Kevin Carter, OGC

At NSLB/OGC's request - WFO reviewed the nature of our relationship with [redacted] Based on contact with the WFO squad (A-2) that serves orders to [redacted] and the supervisors of that program - WFO identified no systemic or pervasive problems with [redacted] compliance. IA [redacted] was specifically contacted and she advised that her relationship with [redacted] is excellent. WIth respect to the specific FISA order you identified, WFO determined that the delay was due to a initial misreading of the order by [redacted] which was rectified when brought to their attention. If FBIHQ learns of other information suggesting that problems exist - WFO will promptly address as they are reported to WFO. Again - because [redacted] is an important WFO liaison contact - it is the ADIC WFO policy that any complaints or concerns relating to [redacted] be handled in coordination with WFO.

b6
b7C

The WFO POCs for issues concerning [redacted] are WFO Administrative ASAC (Brian Fortin - acting) for administrative or problem matters, CDC [redacted] for legal issues, and supervisor [redacted] (A-2) for service issues.

Finally - [redacted] is well aware of the delay in the DOJ processing of FISA orders and they will be the first to point out that they usually receive FISA orders significantly after the date signed by the FISC.

[redacted]
WFO Office of Division Counsel [redacted]

b2
b6
b7C

~~Privileged and Confidential~~

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Monday, August 23, 2004 5:19 PM b6
To: [redacted] (OGC) (FBI) b7C
Subject: 2702 Issue

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] Can you help with a matter of concern to [redacted] He believes that the [redacted] is an invaluable resource to the Bureau. He therefore likes to try and help [redacted] whenever he can. From time to time, [redacted] pass along [redacted] The threat is potential loss of life from an attack. [redacted] has been complaining that [redacted] provides great service but [redacted] is problematic in tha [redacted] b2 b7E b6 b7C b7D

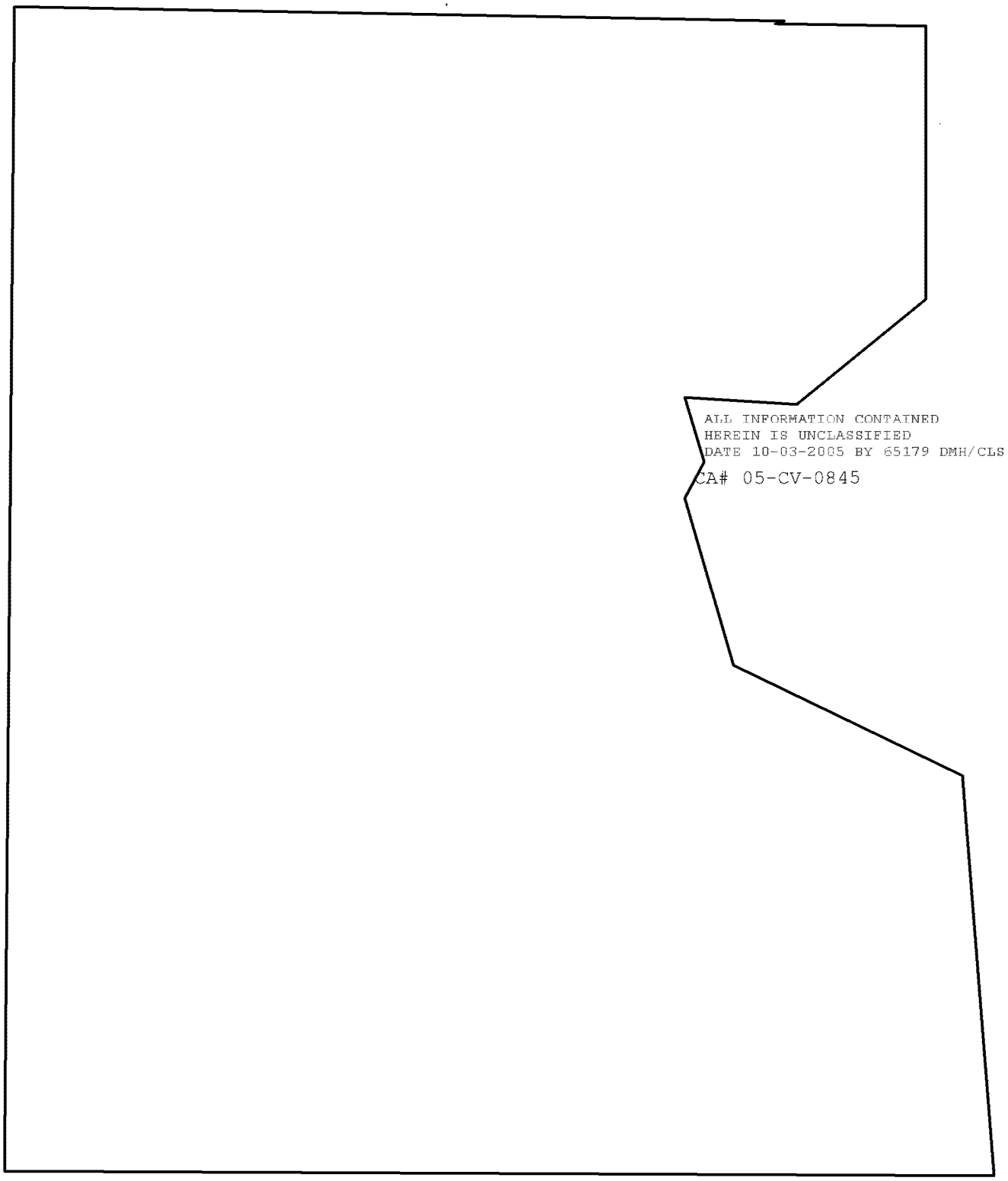
Can you please follow up on this in a few ways? Talk to [redacted] (I spoke with him once about this) and see what information he has abou [redacted] compliance. You may also want to speak with [redacted] to see what knowledge they may have about compliance. Second, I'm a bit concerned that this may be a misuse of 2702 authority. If the requests from [redacted] have a clear nexus to FBI cases and they are bona fide emergencies, then I am okay with it. If, however, we are doing this purely for [redacted] and doing it fo [redacted] on a routine basis, then I think it could be a problem. [redacted] of ILU has issued some guidance on 2702. See me if you do not have it. Can you do some research on 2702 (in addition to finding out what the problems are with [redacted] and prepare a memo for [redacted] on proper use of the tool, including whatever you find out abou [redacted] Please let me know if you have any questions. Thanks.

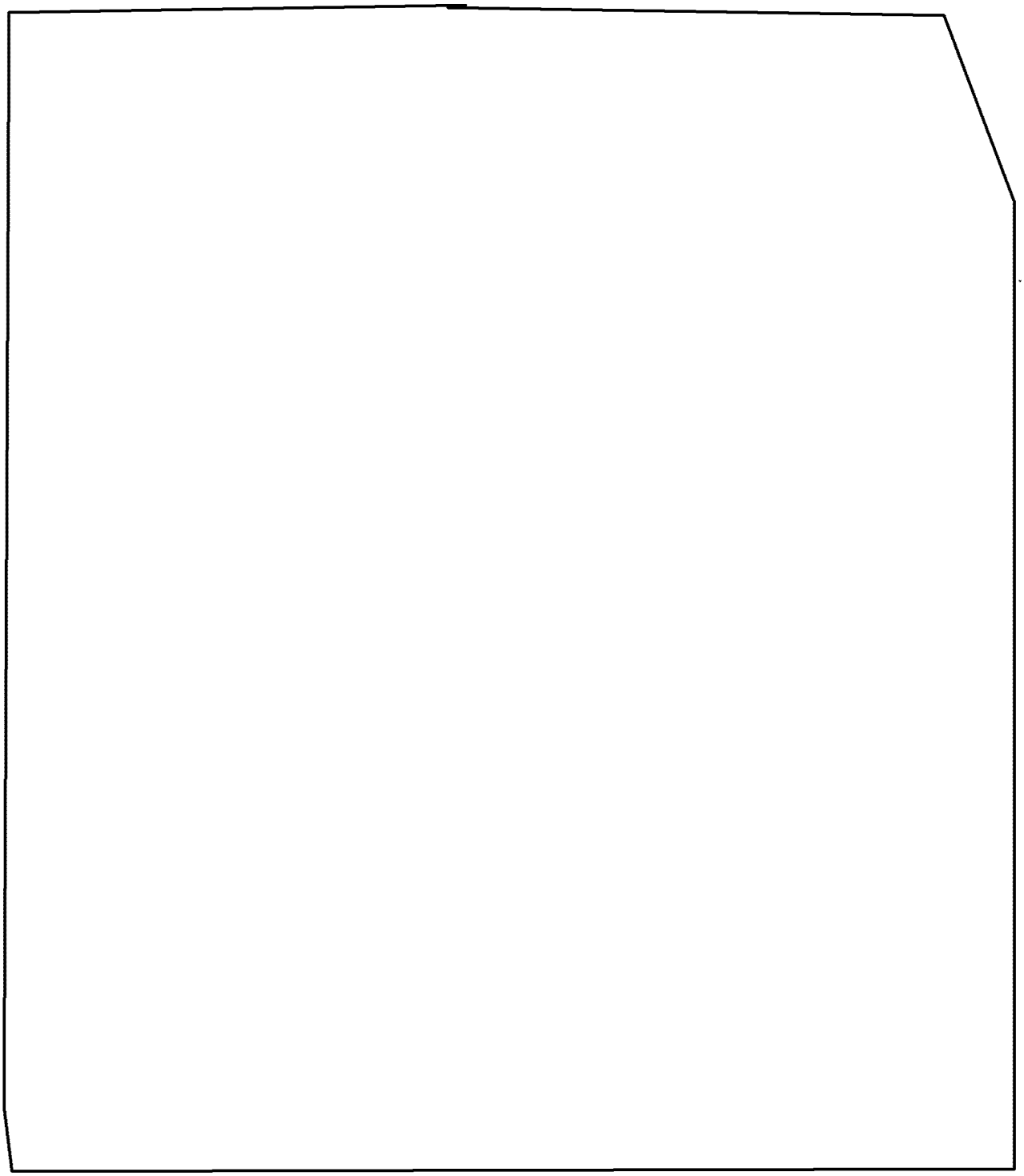
SENSITIVE BUT UNCLASSIFIED

b5
b6
b7C

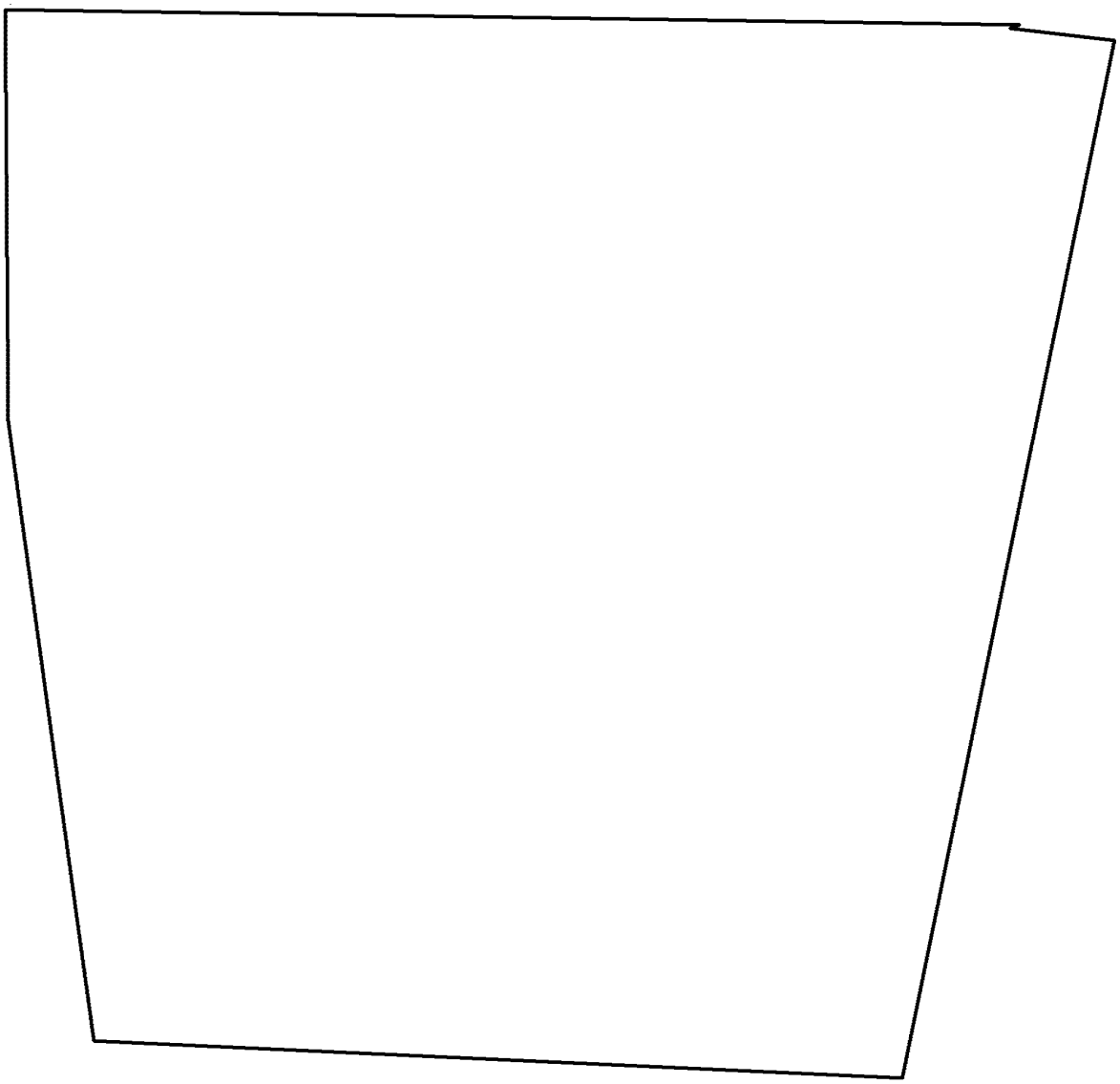
(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

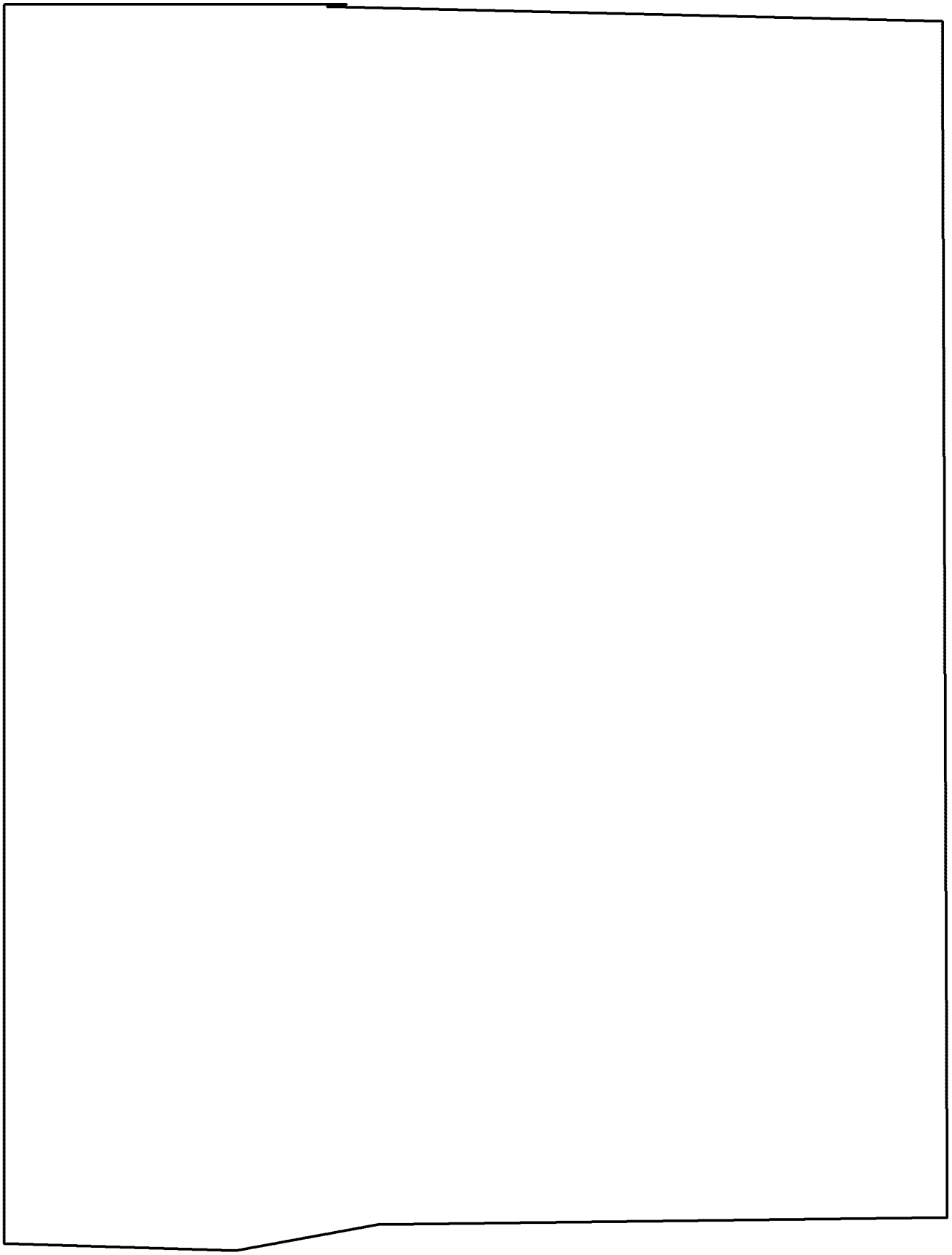




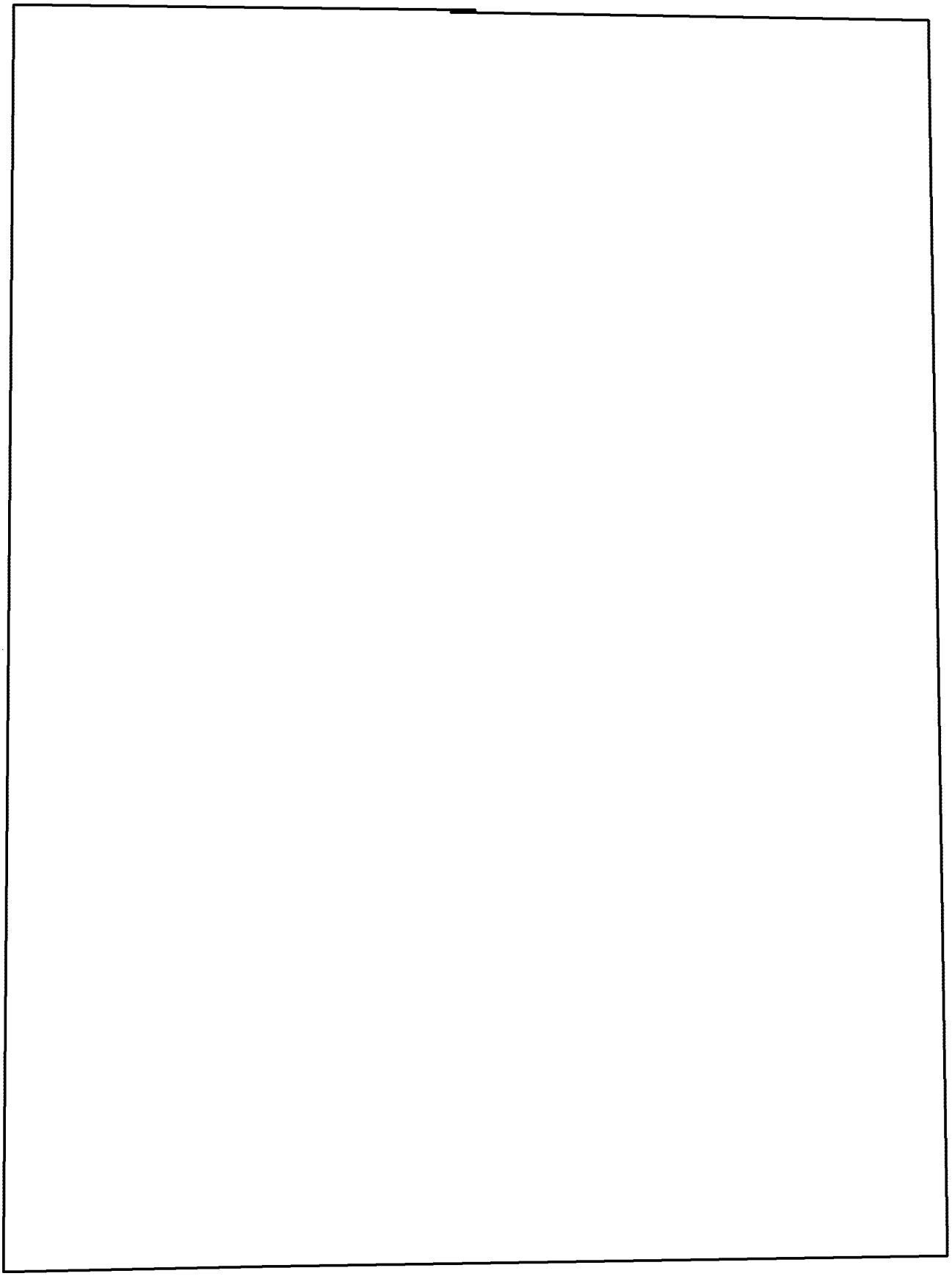
b5
b6
b7C



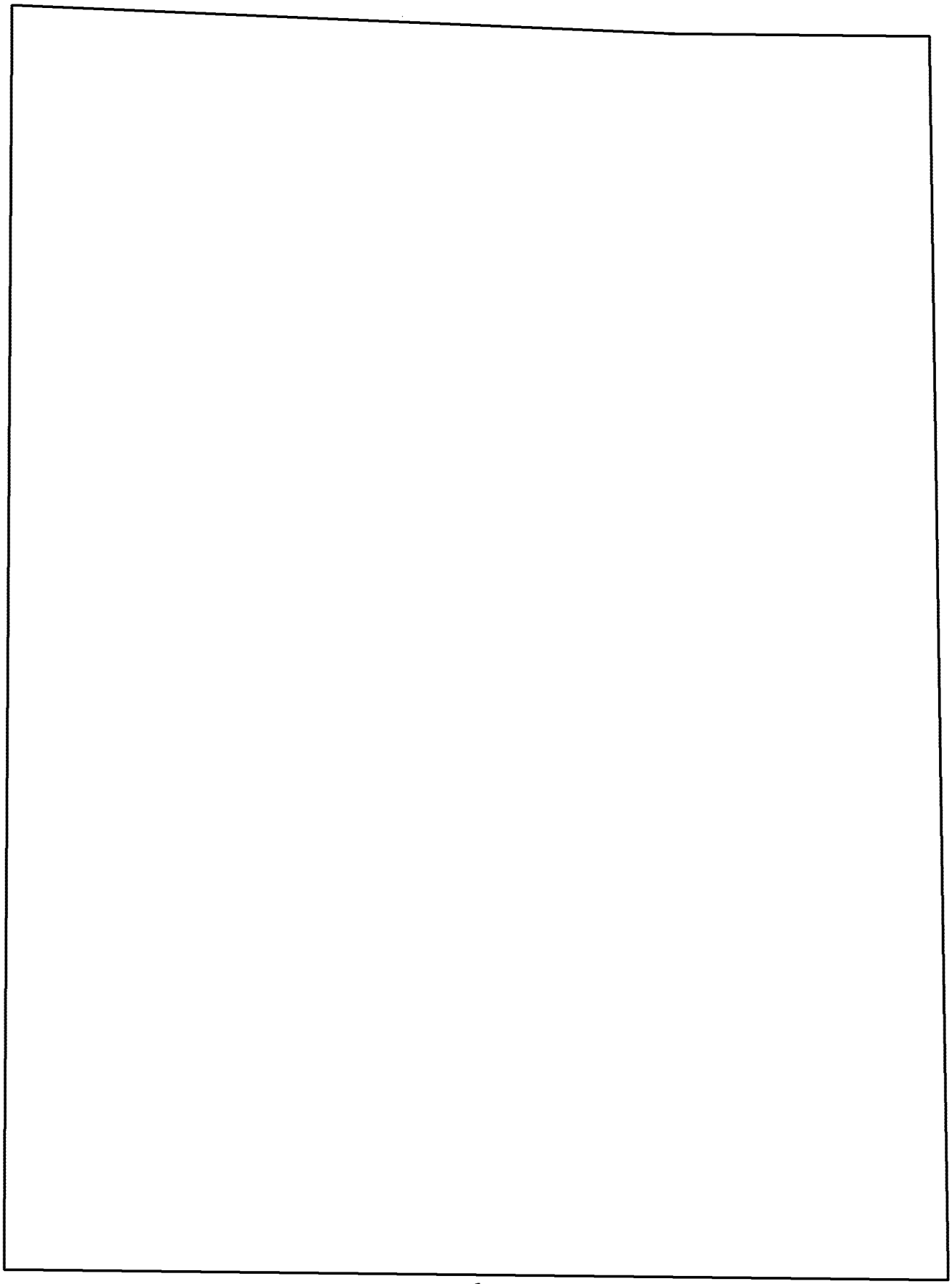
b5
b6
b7C



b5

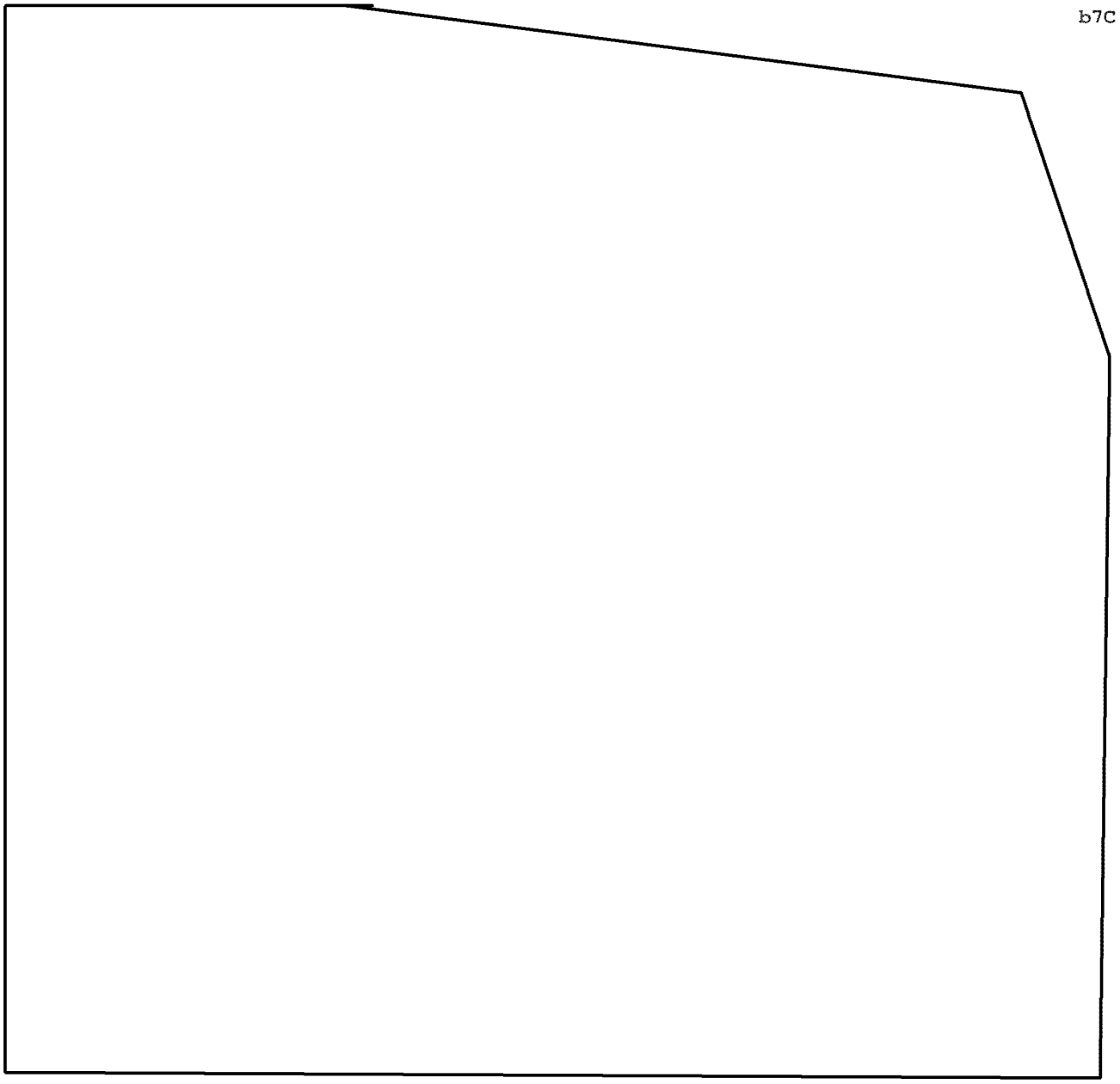


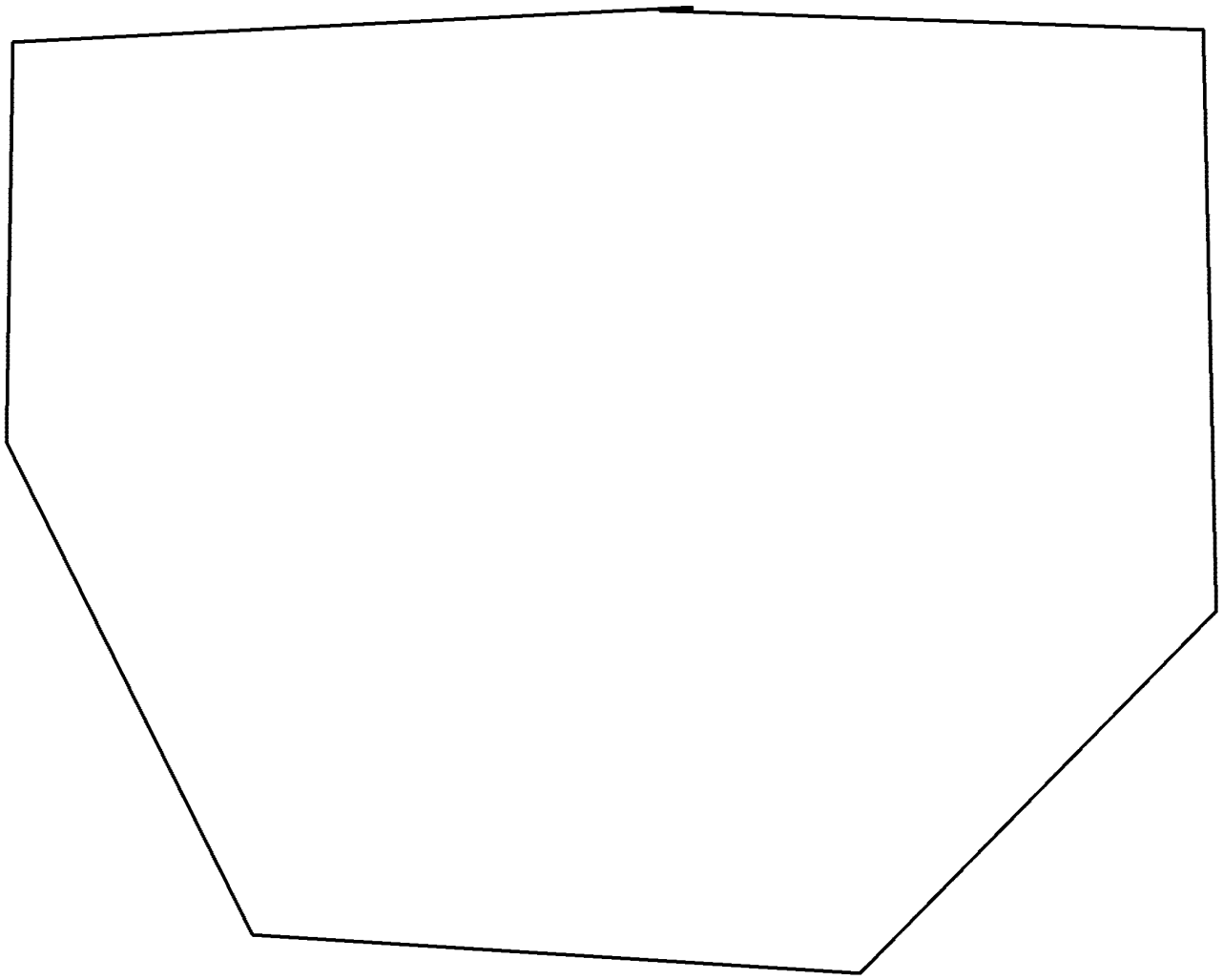
b5



In Reply, Please Refer to
File No.

b5
b6
b7C





b6
b7C

[redacted] (OGC) (FBI)

From: [redacted] (Div13) (FBI)
Sent: Monday, May 10, 2004 7:09 AM
To: [redacted] (Div09) (FBI)
Subject: RE: Question on dissem of Grand Jury info to OIPR

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Is a certain person at OIPR getting LHM's with FGJ info? The AUSA was looking for a specific name to add to the list. I said I'd check.

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Wednesday, May 05, 2004 1:28 PM
To: [redacted] (Div13) (FBI)
Subject: RE: Question on dissem of Grand Jury info to OIPR

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Yes, but this is disclosure of GJ info and according to the AGG (see EC from OGC dated 11/5/02) it must be marked if it identifies a USPER by name, nickname, etc. Most LHMs to OIPR don't contain GJ info. Yes, the AUSA has to notify the judge that the info will be shared with OIPR.

-----Original Message-----
From [redacted] (Div13) (FBI)
Sent: Wednesday, May 05, 2004 10:07 AM
To: [redacted] (Div09) (FBI)
Subject: RE: Question on dissem of Grand Jury info to OIPR

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

yes there is usper info, but we send usper info to OIPR all the time, thousands of LHMs.

So do we need the AUSA to pre-approve the diseminaton of the FGJ info to OIPR?

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Wednesday, May 05, 2004 10:03 AM
To: [redacted] Div13) (FBI)
Subject: RE: Question on dissem of Grand Jury info to OIPR

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Does the info in the LHM identify any USPER by name, etc.? If so, the info will have to marked as containing USPER info.

In addition, the AUSA will have to notify the court that GJ info is being disseminated to OIPR.

-----Original Message-----
From: [redacted](Div13) (FBI) b6
Sent: Wednesday, May 05, 2004 9:31 AM b7C
To: [redacted](Div09) (FBI)
Subject: RE: Question on dissem of Grand Jury info to OIPR

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

The LHM is the initiation of a PI notification.

-----Original Message-----
From: [redacted](Div09) (FBI) b6
Sent: Wednesday, May 05, 2004 9:24 AM b7C
To: [redacted](Div13) (FBI)
Subject: RE: Question on dissem of Grand Jury info to OIPR

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Is this for an initiation or an annual LHM?

-----Original Message-----
From [redacted] (Div13) (FBI) b6
Sent: Wednesday, May 05, 2004 8:01 AM b7C
To: [redacted](Div09) (FBI)
Subject: Question on dissem of Grand Jury info to OIPR

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

We have received an OIPR [redacted] in the matter were obtained via Grand Jury supoena. The paragraph goes on to quote [redacted]

Can this LHM be sent to OIPR with that grand jury info in it? b2 b7E

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

DATE: 10-19-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 10-19-2030

CA# 05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] OGC) (FBI)

From: [redacted] (CTD) (FBI) ~~SECRET~~

Sent: Thursday, August 05, 2004 12:13 PM

To: [redacted] (SI) (FBI) b6

Cc: [redacted] b7C

Subject: RE: a pending pen application

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b5 b6 b7C

SSA [redacted]
FBIHQ / CTD / ITOS II / PRGU
[redacted] (o)
[redacted] (p) b6 b7C

-----Original Message-----
From [redacted] SI) (FBI)
Sent: Thursday, August 05, 2004 11:47 AM
To: [redacted] (CTD) (FBI); [redacted] (CTD) (FBI)
Cc: [redacted] OGC) (FBI); [redacted] (SI) (FBI)
Subject: RE: a pending pen application

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b5 b6 b7C

Thanks, [redacted]

SA [redacted]
Springfield Division, Champaign RA
[redacted] b6 ~~SECRET~~

-----Original Message----- b7C
From: [redacted] (CTD) (FBI)

Sent: Thursday, August 05, 2004 9:33 AM SECRET
To: (CTD) (FBI)
Cc: (OGC) (FBI) SI) (FBI)
Subject: FW: a pending pen application

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

a.k.a. Mr. Pen Register) -

b6
b7C

Please contact case agent SA and obtain an update re how FBI Springfield has handled the collection on this PR/TT. What is the current status?

b5
b6
b7C

I dunno. ourt-authorized data obtained via an application which contained one (1) non-material good-faith error seems draconian to me. I do not think we should accept this remedy without serious discussion and consideration.

Thanks.

SSA
FBIHQ / CTD / ITOS II / PRGU
(o)
(p)

b2
b6
b7C

-----Original Message-----
From: (OGC) (OGA)
Sent: Thursday, August 05, 2004 9:54 AM
To: (CTD) (FBI); (SI) (FBI)
Subject: a pending pen application

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S)

b1
b5
b6
b7C

I can be reached at at OIPR (voice mail) or at the FBI at (no voice mail).

b7A

hope your move went well.

b2
b6
b7C

SECRET
SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

SA
Springfield Division, Champaign RA

b6
b7C

-----Original Message-----
From: (OGC) (FBI)
Sent: Monday, August 09, 2004 2:50 PM
To (SI) (FBI)
Subject: RE: Pending pen register

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Thanks, that's helpful. When did you learn about the need to change the subject's status? Also, do you happen to know why this has not been brought to the attention of the court for so long? Is it because the OIPR attorney was not able to have draft explanations to the court approved by James Baker? It sounds to me like you and FBIHQ passed along the information to OIPR in a timely fashion, but the delay in getting it to court is due to the situation at OIPR. Correct?

b6
b7C

-----Original Message-----
From: (SI) (FBI)
Sent: Monday, August 09, 2004 3:43 PM
To: (OGC) (FBI)
Subject: RE: Pending pen register

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

(S)

b1
b6
b7C
b3
b7A

SA
Springfield Division, Champaign RA

-----Original Message-----
From: (OGC) (FBI)
Sent: Monday, August 09, 2004 2:33 P
To: SI) (FBI)
Subject: Pending pen register

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

~~SECRET~~

~~SECRET~~

b1 [redacted] is out on SL today and [redacted] (S)
b5 [redacted]
b7A [redacted]
b6 [redacted]
b7C [redacted]

Thanks,

[redacted]

NSLB

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI) ~~SECRET~~

From: [redacted] (Div13) (FBI)
Sent: Monday, May 10, 2004 10:31 AM
To: [redacted] (Div09) (FBI)
Subject: RE: Pen register

DATE: 10-14-2005 b6
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C) b7C
DECLASSIFY ON: 10-14-2030
CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Okay, so if I understand it right. . . You approve of us sending it on to OIPR?

Thanks

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Monday, May 10, 2004 10:28 AM
To: [redacted] (Div13) (FBI) b6
Subject: RE: Pen register b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I really should take a look at those in the draft stage so that I can identify any potential legal issues prior to the application being sent to OIPR. Plus, under the new system I should be reviewing things before they are assigned to an OIPR attorney. After they are assigned, my role is limited. I intend to send something on procedures under this new system to everyone in PRGU soon. b6 b7C

[redacted]

-----Original Message-----
From: [redacted] (Div13) (FBI) b6
Sent: Monday, May 10, 2004 10:18 AM
To: [redacted] (Div09) (FBI) b7C
Subject: FW: Pen register

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

This is in regards to the email you sent [redacted] We will get it to OIPR this week.

You won't need to do anything on it until OIPR gets through with it. Unless . . . according to the new AG thing, do you stick close to Pen Registers or not?

Thanks b6 b7C

[redacted]

-----Original Message-----
From: [redacted] (Div13) (FBI)
Sent: Monday, May 10, 2004 10:15 AM b6
To: [redacted] (Div13) (FBI)

~~SECRET~~ b7C

SECRET

Subject: RE: Pen register

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

You can start on it. Touch base with [redacted] and let him know we are on it. It is one that we should go up on. He is the main guy in [redacted]

b2
b7E
b6
b7C

-----Original Message-----
From: [redacted] Div13) (FBI)
Sent: Monday, May 10, 2004 9:54 AM
To: [redacted] (Div13) (FBI)
Subject: RE: Pen register

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Good lord, [redacted] on it this week. I just got the application on Friday. The EC was dated 4/20. I haven't read it yet. Do you want to see it. And yes, I'll get it in the DB.

-----Original Message-----
From [redacted] (Div13) (FBI)
Sent: Monday, May 10, 2004 9:49 AM
To: [redacted] (Div13) (FBI)
Subject: FW: Pen register

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] do you remember this request? It is possible that it happened while you were gone. If you don't remember it, I will check with [redacted] Thanks. D

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Monday, May 10, 2004 9:38 AM
To: [redacted] (Div13) (FBI)
Subject: Pen register

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

SECRET

Hi [redacted]

I received an EC from [redacted] dated 4/20/04, requesting [redacted] (S) [redacted] reviewed the request form and it is legally sufficient. Do you need me to do anything else on that?

[redacted]

b1
b2
b7E
b6
b7C

SECRET

SECRET

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI) b6 b7C

From: [redacted] (CTD) (FBI)
Sent: Wednesday, September 01, 2004 12:14 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] OGC) (FBI)
Subject: [redacted] (S)

DATE: 10-17-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 10-17-2030
CA# 05-CV-0845

b1

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SECRET
RECORD [redacted] (S)

[redacted] I just got thi[redacted], which we hope is in final form [redacted] (S)
(S) [redacted]

I'm working with [redacted] at OIPR on this, so if you could include him on the results, he should be able to get this t[redacted] on Friday.

b1 b2 b7E b6 b7C

Thanks,

[redacted]
SSA [redacted]
[redacted]

b2 b7E b6 b7C

DERIVED FROM: Multiple Sources
DECLASSIFY ON: 20290901
SECRET

SECRET

[redacted] (OGC) (FBI)

b6
b7C

From: [redacted] (Div09) (FBI)
Sent: Wednesday, March 24, 2004 11:31 AM
To: [redacted] (Div09) (FBI)
Subject: RE: obtaining tax info

UNCLASSIFIED
NON-RECORD

[redacted]

b5

But you can review the relevant sections yourself and see if you find something that I overlooked.

[redacted]

b6
b7E

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Wednesday, March 24, 2004 9:46 AM
To: [redacted] (Div09) (FBI)
Subject: RE: obtaining tax info

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C
b5

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Wednesday, March 24, 2004 9:42 AM
To: [redacted] Div09) (FBI)
Subject: RE: obtaining tax info

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C
b5
b2
b7E

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Tuesday, March 23, 2004 3:51 PM
To: [redacted] (Div09) (FBI)
Subject: obtaining tax info

b6
b7C
b2
b7E
b5

UNCLASSIFIED
NON-RECORD

[redacted]

Thanks.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

(Revised 11/04/2003)

FBI FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)
BUSINESS RECORDS REQUEST FORM

INSTRUCTIONS

The FBI must use this form to request that the National Security Law Branch (NSLB) prepare an application to the Foreign Intelligence Surveillance Court (FISC) for a Business Records Order, pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §1861.

FBI field offices must adhere to the following procedures in using this form:

(1) The FBI special agent (SA) in the relevant FBI field office/division with primary responsibility for the foreign counterintelligence or counterterrorism investigation to which the request relates should complete this form.

(2) This form must be reviewed and approved by Supervisory Special Agent (SSA), the Chief Division Counsel (CDC), and the Special Agent in Charge (SAC) or the Program Assistant Special Agent-in-Charge(ASAC).

(3) This form should be sent to the appropriate FBI Headquarters division (Counterintelligence or Counterterrorism), the National Security Law Branch (NSLB), Room 7975, and the FISA Unit, Room 1B046.

Based on the information provided on this form, NSLB will prepare a FISA Business Records Application, and Order and present it to the FISC.

Direct any questions about how to complete this form to the FBI HQ SSA or NSLB (202) 324-3951.

Blank versions of this form are unclassified. **Add classification markings to the form according to the classification of the information you provide.**

(Classification of completed form)

(Revised 11/04/03)

FISA REQUEST FOR ACCESS TO BUSINESS RECORDS, I.E., "ANY TANGIBLE THING (INCLUDING BOOKS, RECORDS, PAPERS, DOCUMENTS AND OTHER ITEMS)" (50 USC Section 1861)

1. **General Information**

   a. **Name of Subject(s) of the investigation for which the tangible things are sought:**

   b. **FBI file number(s):**

   c. **Date full investigation or preliminary investigation of such subject was authorized:**

   d. **Office of origin:**

   e. **Case Agent Point of Contact:**
      i. **Name:**
      ii. **Telephone:**
      iii. **Secure Fax:**

   f. **FBI Headquarters SSA:**
      i. **Name:**
      ii. **Telephone:**
      iii. **Secure Fax:**

   g. **Status of Subject of the Investigation**
      i. **USP**
      ii. **Non-USP or**
      iii. **Foreign power**

   h. **Status of Subject of the Request, if different from Subject of the Investigation**
      i. **USP**
      ii. **Non-USP**
      iii. **Foreign Power**

2. **Basis of Request for Tangible Things**

   a. **Specifically describe the tangible things (e.g. books, records, papers, documents) you are requesting. If the tangible thing is not a written document (e.g., an apartment key), explain why you believe that it is being kept by a custodian in the normal course of business. Note that the subject of the request does not have to**

be the subject of the investigation.

b. If relevant, state whether you are requesting the original or copy of the tangible things.

c. Provide a brief summary of the full investigation or preliminary investigation for which the requested tangible things are sought.

d. Explain the manner in which the requested tangible things are expected to provide foreign intelligence information for the full investigation or preliminary investigation.

3. Service of the Business Records Order

a. Identify the current custodian, owner, or person in possession of the requested tangible things.

b. Identify the name, address, title, and telephone number of any custodian or person to whom an order needs to be directed to require the production of the requested tangible things.

4. Field Office Approval

I have reviewed this request and certify that the requested tangible things are sought for an authorized investigation, conducted in accordance with the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations, to obtain foreign intelligence not concerning a USPER or to protect against international terrorism or clandestine intelligence activities. I further certify that the authorized investigation is not being conducted solely upon the basis of activities protected by the First Amendment of the Constitution.

Supervisory Special Agent (SSA) approving this form:
Printed (or Typed) Name:
Telephone Number:

Signature: **Date:**

(Classification of completed form)

CDC approving this form:
Printed (or Typed) Name:
Telephone Number:

Signature: **Date:**

SAC or Program ASAC approving this form:
Printed (or Typed) Name:
Telephone Number:

Signature: **Date:**

(Classification of completed form)

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 8
Page 157 ~ Referral/Direct
Page 158 ~ Referral/Direct
Page 159 ~ Referral/Direct
Page 160 ~ Referral/Direct
Page 161 ~ Referral/Direct
Page 162 ~ Referral/Direct
Page 163 ~ Referral/Direct
Page 164 ~ Referral/Direct

Order Code RL31377

The USA PATRIOT Act: A Legal Analysis

April 15, 2002

Charles Doyle
Senior Specialist
American Law Division

The USA PATRIOT Act: A Legal Analysis

Summary

The USA PATRIOT Act passed in the wake of the September 11 terrorist attacks. It flows from a consultation draft circulated by the Department of Justice, to which Congress made substantial modifications and additions. The stated purpose of the Act is to enable law enforcement officials to track down and punish those responsible for the attacks and to protect against any similar attacks.

The Act grants federal officials greater powers to trace and intercept terrorists' communications both for law enforcement and foreign intelligence purposes. It reenforces federal anti-money laundering laws and regulations in an effort to deny terrorists the resources necessary for future attacks. It tightens our immigration laws to close our borders to foreign terrorists and to expel those among us. Finally, it creates a few new federal crimes, such as the one outlawing terrorists' attacks on mass transit; increases the penalties for many others; and institutes several procedural changes, such as a longer statute of limitations for crimes of terrorism.

Critics have suggested that it may go too far. The authority to monitor e-mail traffic, to share grand jury information with intelligence and immigration officers, to confiscate property, and to impose new book-keeping requirements on financial institutions, are among the features troubling to some.

The Act itself responds to some of these reservations. Many of the wiretapping and foreign intelligence amendments sunset on December 31, 2005. The Act creates judicial safeguards for e-mail monitoring and grand jury disclosures; recognizes innocent owner defenses to forfeiture; and entrusts enhanced anti-money laundering powers to those regulatory authorities whose concerns include the well being of our financial institutions.

This report, stripped of its citations and footnotes, is available in an abbreviated form as *The USA PATRIOT Act: A Sketch*, CRS REP.NO. RS21203. In addition, much of the information contained here may also be found under a different arrangement in a report entitled, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, CRS REP.NO. RL31200 (Dec. 10, 2001). A wider array of terrorism-related analysis appears on the CRS terrorism electronic briefing book page.

Contents

The USA PATRIOT Act: A Legal Analysis

Introduction

Congress passed the USA PATRIOT Act (the Act) in response to the terrorists' attacks of September 11, 2001.[1] The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. It vests the Secretary of the Treasury with regulatory powers to combat corruption of U.S. financial institutions for foreign money laundering purposes. It seeks to further close our borders to foreign terrorists and to detain and remove those within our borders. It creates new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists. Although it is not without safeguards, critics contend some of its provisions go too far. Although it grants many of the enhancements sought by the Department of Justice, others are concerned that it does not go far enough.

The Act originated as H.R.2975 (the PATRIOT Act) in the House and S.1510 in the Senate (the USA Act).[2] S.1510 passed the Senate on October 11, 2001, 147 *Cong.Rec.* S10604 (daily ed.). The House Judiciary Committee reported out an amended version of H.R. 2975 on the same day, H.R.Rep.No. 107-236. The House passed H.R. 2975 the following day after substituting the text of H.R. 3108, 147 *Cong.Rec.* H6775-776 (daily ed. Oct. 12, 2001). The House-passed version incorporated most of the money laundering provisions found in an earlier House bill, H.R. 3004, many of which had counterparts in S.1510 as approved by the Senate.[3] The House subsequently passed a clean bill, H.R. 3162 (under suspension of the rules), which resolved the differences between H.R. 2975 and S.1510, 147 *Cong.Rec.* H7224 (daily ed. Oct. 24, 2001). The Senate agreed, 147 *Cong.Rec.* S10969 (daily

---

[1] P.L. 107-56, 115 Stat. 272 (2001); its full title is the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)."

[2] H.R. 2975 was introduced by Representative Sensenbrenner for himself and Representatives Conyers, Hyde, Coble, Goodlatte, Jenkins, Jackson-Lee, Cannon, Meehan, Graham, Bachus, Wexler, Hostettler, Keller, Issa, Hart, Flake, Schiff, Thomas, Goss, Rangel, Berman and Lofgren; S.1510 by Senator Daschle for himself and Senators Lott, Leahy, Hatch, Graham, Shelby and Sarbanes.

[3] H.R. 3004 was introduced by Representative Oxley for himself and Represenatives LaFalce, Leach, Maloney, Roukema, Bentsen, Hooley, Bereuter, Baker, Bachus, King, Kelly, Gillmore, Cantor, Riley, Latourette, Green (of Wisconsin), and Grucci; and reported out of the House Financial Services Committee with amendments on October 15, 2001, H.R.Rep.No. 107-250. H.R. 3004, as reported out, included Internet gambling amendments that were not included in H.R. 2975/H.R.3108.

ed. Oct. 24, 2001), and H.R. 3162 was sent to the President who signed it on October 26, 2001.

Criminal Investigations: Tracking and Gathering Communications

A portion of the Act addresses issues suggested originally in a Department of Justice proposal circulated in mid-September.[4] The first of its suggestions called for amendments to federal surveillance laws, laws which govern the capture and tracking of suspected terrorists' communications within the United States. Federal law features a three tiered system, erected for the dual purpose of protecting the confidentiality of private telephone, face-to-face, and computer communications while enabling authorities to identify and intercept criminal communications.[5]

The tiers reflected the Supreme Court's interpretation of the Fourth Amendment's ban on unreasonable searches and seizures.[6] The Amendment protects private conversations, *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967). It does not cloak information, even highly personal information, for which there is no individual justifiable expectation of privacy, such as telephone company records of calls made to and from an individual's home, *Smith v. Maryland*, 442 U.S. 735 (1979), or bank records of an individual's financial dealings, *United States v. Miller*, 425 U.S. 435 (1976).

Congress responded to *Berger* and *Katz*, with Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2522 (Title III). Title III, as amended, generally prohibits electronic eavesdropping on telephone conversations, face-to-face conversations, or computer and other forms of electronic communications, 18 U.S.C. 2511.[7] At the same time, it gives authorities a narrowly defined process for electronic surveillance to be used as a last resort in serious

---

[4] The Department's proposal, dated September 20, 2001, came with a brief section by section analysis. Both the proposal (*Draft*) and analysis (*DoJ*) were printed as an appendix in *Administration's Draft Anti-Terrorism Act of 2001, Hearing Before the House Comm. on the Judiciary*, 107th Cong., 1st Sess. 54 (2001).

[5] For a general discussion of federal law in the area prior to enactment of the Act, *see*, Stevens & Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretappping and Electronic Eavesdropping*, CRS REP.NO. 98-327A (Aug. 8, 2001); Fishman & McKenna, WIRETAPPING AND EAVESDROPPING (2d ed. 1995 & 2001 Supp.).

[6] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized," *U.S. Const.* Amend. IV.

[7] Although there are technical differences, the interception processes are popularly known as wiretapping, electronic eavesdropping, or electronic surveillance. The terms are used interchangeable here for purposes of convenience, but strictly speaking, wiretapping is limited to the mechanical or electronic interception of telephone conversations, while electronic eavesdropping or electronic surveillance refers to mechanical or electronic interception of communications generally.

criminal cases. When approved by senior Justice Department officials,[8] law enforcement officers may seek a court order authorizing them to secretly capture conversations concerning any of a statutory list of offenses (predicate offenses), 18 U.S.C. 2516.[9]

---

[8] "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of" one or more predicate offense, 18 U.S.C. 2516.

[9] The predicate offense list includes (a) felony violations of 42 U.S.C. 2274 through 2277 (enforcement of the Atomic Energy Act of 1954), 42 U.S.C. 2284 (sabotage of nuclear facilities or fuel), or of 18 U.S.C. ch. 37 (espionage), ch. 90 (protection of trade secrets), ch. 105 (sabotage), ch. 115 (treason), ch. 102 (riots), ch. 65 (malicious mischief), ch. 111 (destruction of vessels), or ch. 81 (piracy); (b) a violation of 29 U.S.C. 186 or 501(c) (restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under title 18 of the United States Code; (c) any offense which is punishable under 18 U.S.C. 201 (bribery of public officials and witnesses), 215 (bribery of bank officials), 224 (bribery in sporting contests), 844 (d), (e), (f), (g), (h), or (i) (unlawful use of explosives), 1032 (concealment of assets), 1084 (transmission of wagering information), 751 (escape), 1014 (loans and credit applications generally; renewals and discounts), 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), 1510 (obstruction of criminal investigations), 1511 (obstruction of State or local law enforcement), 1751 (presidential and presidential staff assassination, kidnaping, or assault), 1951 (interference with commerce by threats or violence), 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), 1958 (use of interstate commerce facilities in the commission of murder for hire), 1959 (violent crimes in aid of racketeering activity), 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), 1955 (prohibition of business enterprises of gambling), 1956 (laundering of monetary instruments), 1957 (engaging in monetary transactions in property derived from specified unlawful activity), 659 (theft from interstate shipment), 664 (embezzlement from pension and welfare funds), *1030 (computer abuse felonies)*, 1343 (fraud by wire, radio, or television), 1344 (bank fraud), 2251 and 2252 (sexual exploitation of children), 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), 2321 (trafficking in certain motor vehicles or motor vehicle parts), 1203 (hostage taking), 1029 (fraud and related activity in connection with access devices), 3146 (penalty for failure to appear), 3521(b)(3) (witness relocation and assistance), 32 (destruction of aircraft or aircraft facilities), 38 (aircraft parts fraud), 1963 (violations with respect to racketeer influenced and corrupt organizations), 115 (threatening or retaliating against a Federal official), 1341 (mail fraud), 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnaping, or assault), 831 (prohibited transactions involving nuclear materials), 33 (destruction of motor vehicles or motor vehicle facilities), 175 (biological weapons), 1992 (wrecking trains), a felony violation of 1028 (production of false identification documentation), 1425 (procurement of citizenship or nationalization unlawfully), 1426 (reproduction of naturalization or citizenship papers), 1427 (sale of naturalization or citizenship papers), 1541 (passport issuance without authority), 1542 (false statements in passport applications), 1543 (forgery or false use of passports), 1544 (misuse of passports), or 1546 (fraud and misuse of visas, permits, and other documents); (d) any

Title III court orders come replete with instructions describing the permissible duration and scope of the surveillance as well as the conversations which may be seized and the efforts to be taken to minimize the seizure of innocent conversations, 18 U.S.C. 2518. The court notifies the parties to any conversations seized under the order after the order expires, 18 U.S.C. 2518(8).

Below Title III, the next tier of privacy protection covers some of those matters which the Supreme Court has described as beyond the reach of the Fourth Amendment protection – telephone records, e-mail held in third party storage, and the like, 18 U.S.C. 2701-2709 (Chapter 121). Here, the law permits law enforcement access, ordinarily pursuant to a warrant or court order or under a subpoena in some cases, but in connection with *any* criminal investigation and without the extraordinary levels of approval or constraint that mark a Title III interception, 18 U.S.C. 2703.

Least demanding and perhaps least intrusive of all is the procedure that governs court orders approving the government's use of trap and trace devices and pen registers, a kind of secret "caller id", which identify the source and destination of calls made to and from a particular telephone, 18 U.S.C. 3121-3127 (Chapter 206). The orders are available based on the government's certification, rather than a finding of the court, that the use of the device is likely to produce information relevant to the investigation of a crime, any crime, 18 U.S.C. 3123. The devices record no more than the identity of the participants in a telephone conversation,[10] but neither the orders nor the results they produce need ever be revealed to the participants.

The Act modifies the procedures at each of the three levels. It:

---

offense involving counterfeiting punishable under 18 U.S.C. 471, 472, or 473; (e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States; (f) any offense including extortionate credit transactions under 18 U.S.C. 892, 893, or 894; (g) a violation of 31 U.S.C. 5322 (dealing with the reporting of currency transactions); (h) any felony violation of 18 U.S.C. 2511 and 2512 (interception and disclosure of certain communications and to certain intercepting devices); (i) any felony violation of 18 U.S.C. ch. 71 (obscenity); (j) 49 U.S.C. 60123(b) (destruction of a natural gas pipeline), 46502 (aircraft piracy); (k) 22 U.S.C. 2778 (Arms Export Control Act); (l) the location of any fugitive from justice from an offense described in this section; (m) a violation of 8 U.S.C. 1324, 1327, or 1328; (n) any felony violation of 18 U.S.C. 922, 924 (firearms); (o) any violation of 26 U.S.C. 5861 (firearms); (p) a felony violation of 18 U.S.C. 1028 (production of false identification documents), 1542 (false statements in passport applications), 1546 (fraud and misuse of visas, permits, and other documents) or a violation of 8 U.S.C. 1324, 1327, or 1328 (smuggling of aliens); *(p) 229 (chemical weapons), 2332 (terrorist violence against Americans overseas), 2332a (weapons of mass destruction), 2332b (multinational terrorism), 2332d (financial transactions with countries supporting terrorism), 2339A (support of terrorist), 2332B (support of terrorist organizations);* (r) any conspiracy to commit any of these, 18 U.S.C. 2516(1)(crimes added by the Act in italics). Other than telephone face to face conversations (*i.e.*, electronic communications), the approval of senior Justice Department officials is not required and an order may be sought in any felony investigation, 18 U.S.C. 2516(3).

[10] Or more precisely, they reveal no more than the identity of the numbers assigned to the telephone lines activated for a particular communication.

- permits pen register and trap and trace orders for electronic communications (*e.g.*, e-mail)

- authorizes nationwide execution of court orders for pen registers, trap and trace devices, and access to stored e-mail or communication records

- treats stored voice mail like stored e-mail (rather than like telephone conversations)

- permits authorities to intercept communications to and from a trespasser within a computer system (with the permission of the system's owner)

- adds terrorist and computer crimes to Title III's predicate offense list

- reenforces protection for those who help execute Title III, ch. 121, and ch. 206 orders

- encourages cooperation between law enforcement and foreign intelligence investigators

- establishes a claim against the U.S. for certain communications privacy violations by government personnel

- terminates the authority found in many of the these provisions and several of the foreign intelligence amendments with a sunset provision (Dec. 31, 2005).

Pen Registers and Trap and Trace Devices. In section 216, the Act allows court orders authorizing trap and trace devices and pen registers to be used to capture source and addressee information for computer conversations (*e.g.*, e-mail) as well as telephone conversations, 18 U.S.C. 3121, 3123. In answer to objections that e-mail header information can be more revealing than a telephone number, it creates a detailed report to the court, 18 U.S.C. 3123(a)(3).[11]

---

[11] "Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public the agency shall ensure that a record will be maintained which will identify – (i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network; (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and (iv) any information which has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of the such device.

"(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof)," section 216(b)(1).

The use of pen registers or trap and trace devices was limited at one time to the judicial district in which the order was issued, 18 U.S.C. 3123 (2000 ed.). Under section 216, a court with jurisdiction over the crime under investigation may issue an order to be executed anywhere in the United States, 18 U.S.C. 3123(b)(1)(C), 3127(2).[12]

Communications Records and Stored E-Mail. With respect to chapter 126, relating among other things to the content of stored e-mail and to communications records held by third parties, the law permits criminal investigators to retrieve the content of electronic communications in storage, like e-mail, with a search warrant, and if the communication has been in remote storage for more than 180 days without notifying the subscriber, 18 U.S.C. 2703(a),(b). A warrant will also suffice to seize records describing telephone and other communications transactions without customer notice, 18 U.S.C. 2703(c). In the absence of the probable cause necessary for a warrant but with a showing of reasonable grounds to believe that the information sought is relevant to a criminal investigation, officers are entitled to a court order mandating access to electronic communications in remote storage for more than 180 days or to communications records, 18 U.S.C. 2703(b),(c). They can obtain a limited amount of record information (subscribers' names and addresses, telephone numbers, billing records and the like) using an administrative, grand jury, or trial court subpoena, 18 U.S.C. 2703(c)(1)(C). There is no subscriber notification in record cases. Elsewhere, the court may delay customer notification in the face of exigent circumstances or if notice is likely to seriously jeopardize the investigation or unduly delay the trial, 18 U.S.C. 2705.

In order to streamline the investigation process, the Act, in section 210, adds credit card and bank account numbers to the information law enforcement officials may subpoena from a communications service provider's customer records, 18 U.S.C. 2703(c)(1)(C).[13]

Another streamlining amendment, section 220, eliminates the jurisdictional restrictions on access to the content of stored e-mail pursuant to a court order.

---

[12] The Justice Department urged the change in the name of expediency, "At present, the government must apply for new pen trap orders in every jurisdiction where an investigation is being pursued. Hence, law enforcement officers tracking a suspected terrorist in multiple jurisdictions must waste valuable time and resources by obtaining a duplicative order in each jurisdiction," *DoJ* at §101. Here and throughout citations to the United States Code (U.S.C.) without reference to an edition refer to the current Code; references to the 2000 edition of the Code refer to the law prior to amendment by the Act.

[13] Prior to the amendment, "investigators [could] not use a subpoena to obtain such records as credit card number or other form of payment. In many cases, users register with Internet service providers using false names, making the form of payment critical to determining the user's true identity. . . . this information [could] only be obtained by the slower and more cumbersome process of a court order. In fast-moving investigation[s] such as terrorist bombings – in which Internet communications are a critical method of identifying conspirators and in determining the source of the attacks – the delay necessitated by the use of court orders can often be important. Obtaining billing and other information can identify not only the perpetrator but also give valuable information about the financial accounts of those responsible and their conspirators," *DoJ* at §107.

Previously, only a federal court in the district in which the e-mail was stored could issue the order. Under section 220, federal courts in the district where an offense under investigation occurred may issue orders applicable "without geographic limitation," 18 U.S.C. 2703.[14]

The Act, in section 209, treats voice mail like e-mail, that is, subject to the warrant or court order procedure, rather than to the more demanding coverage of Title III once required, *United States v. Smith*, 155 F.3d 1050, 1055-56 (9th Cir. 1998).

Finally, the Act resolves a conflict between chapter 121 and the federal law governing cable companies. Government entities may have access to cable company customer records only under a court order following an adversary hearing if they can show that the records will evidence that the customer is or has engaged in criminal activity, 47 U.S.C. 511(h). When cable companies began offering telephone and other communications services the question arose whether the more demanding cable rules applied or whether law enforcement agencies were entitled to ex parte court orders under the no-notice procedures applicable to communications providers.[15] The Act makes it clear that the cable rules apply when cable television viewing services are

---

[14] Speaking of the law before amendment, DoJ explained, "Current law requires the government to use a search warrant to compel a provider to disclose unopened e-mail. 18 U.S.C. §2703(a). Because Federal Rule of Criminal Procedure 41 requires that the 'property' to be obtained 'be within the district' of the issuing court, however, the rule may not allow the issuance of §2703(a) warrants for e-mail located in other districts. Thus, for example, where an investigator in Boston is seeking electronic e-mail in the Yahoo! account of a suspected terrorist, he may need to coordinate with agents, prosecutors, and judges in the Northern District of California, none of whom have any other involvement in the investigation. This electronic communications information can be critical in establishing relationships, motives, means, and plans of terrorists. Moreover, it is equally relevant to cyber-incidents in which a terrorist motive has not (but may well be) identified. Finally, even cases that require the quickest response (kidnappings, threats, or other dangers to public safety or the economy) may rest on evidence gathered under §2703(a). To further public safety, this section accordingly authorizes courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of their counterparts in other districts where major Internet service providers are located," *DoJ* at §108.

[15] *See e.g., DoJ* at §109 ("Law enforcement must have the capability to trace, intercept, and obtain records of the communications of terrorists and other criminals with great speed, even if they choose to use a cable provider for their telephone and Internet service. This section amends the Cable Communications Policy Act ('Cable Act') to clarify that when a cable company acts as a telephone company or an Internet service provider, it must comply with the same laws governing the interception and disclosure of wire and electronic communications that apply to any other telephone company or Internet service provider. The Cable Act, passed in 1984 to regulate various aspects of the cable television industry, could not take into account the changes in technology that have occurred over the last seventeen years. Cable television companies now often provide Internet access and telephone service in addition to television programming. Because of perceived conflicts between the Cable Act and laws that govern law enforcement's access to communications and records of communications carried by cable companies, cable providers have refused to comply with lawful court orders, thereby slowing or ending critical investigations").

involved and that the communications rules of chapter 121 apply when a cable company or anyone else provides communications services, section 211.

Electronic Surveillance. To Title III's predicate offense list, the Act adds cybercrime (18 U.S.C. 1030) and several terrorists crimes, sections 201, 202.[16] A second cybercrime initiative, section 217, permits law enforcement officials to intercept the communications of an intruder within a protected computer system (*i.e.*, a system used by the federal government, a financial institution, or one used in interstate or foreign commerce or communication), without the necessity of a warrant or court order, 18 U.S.C. 2511(2)(*i*). Yet only the interloper's intruding communications, those to or from the invaded system, are exposed under the section. The Justice Department originally sought the change because the law then did not clearly allow victims of computer trespassing to request law enforcement assistance in monitoring unauthorized attacks as they occur.[17]

Criminal Investigators' Access to Foreign Intelligence Information. The Act clearly contemplates closer working relations between criminal investigators and foreign intelligence investigators, particular in cases of international terrorism.[18] It amends the Foreign Intelligence Surveillance Act (FISA) to that end. As originally enacted, the application for a surveillance order under FISA required certification of the fact that "*the* purpose for the surveillance is to obtain foreign intelligence information," 50 U.S.C. 1804(a)(7)(B)(2000 ed.) (emphasis added), although it anticipated that any evidence divulged as a result might be turned over to law enforcement officials. Defendants often questioned whether authorities had used a FISA surveillance order against them in order to avoid the predicate crime threshold for a Title III order. Out of these challenges arose the notion that perhaps "the purpose" might not always mean the sole purpose. The case law indicated that, while an expectation that evidence of a crime might be discovered did not preclude a FISA order, at such time as a criminal prosecution became the focus of the investigation

---

[16] 18 U.S.C. 229 (chemical weapons), 2332(terrorist acts of violence committed against Americans overseas), 2332a(use of weapons of mass destruction), 2332b(acts of terrorism transcending national boundaries), 2332d(financial transactions with countries which support terrorists), 2339A(providing material support to terrorists), and 2339B(providing material support to terrorist organizations).

[17] "Because service providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves as permitted under current law, they often have no way to exercise their rights to protect themselves from unauthorized attackers. Moreover, such attackers can target critical infrastructures and engage in cyberterrorism," *DoJ* at §106. Elsewhere the Act defines "electronic surveillance" for purposes of the Foreign Intelligence Surveillance Act (FISA) to emphasize that the law enforcement authority for this intruder surveillance does not confer similar authority for purposes of foreign intelligence gathering, section 1003 (50 U.S.C. 1801(f)(2)).

[18] For a general discussion of federal intelligence and law enforcement cooperation, *see*, Best, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, CRS REP.NO. RL30252 (Dec. 3, 2001).

officials were required to either end surveillance or secure an order under Title III.[19]

The Justice Department sought FISA surveillance and physical search authority on the basis of "a" foreign intelligence purpose.[20] Section 218 of the Act insists that foreign intelligence gathering be a "significant purpose" for the request for the FISA surveillance or physical search order, 50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B), a more

---

[19] Before FISA, several lower federal courts recognized a foreign intelligence exception to the Fourth Amendment's warrant clause. It is here that the "primary purpose" notion originated. In *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980), decided after FISA on the basis of pre-existing law, the court declared, "as the district court ruled, the executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons. We think that the district court adopted the proper test, because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution." Subsequent case law, however, is not as clear as it might be: *see e.g., United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984)("FISA permits federal officials to obtain orders authorizing electronic surveillance 'for the purpose of obtaining foreign intelligence information.' The requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of Sec. 1802(b) but also from the requirements in Sec. 1804 as to what the application must contain. The application must contain a certification by a designated official of the executive branch that the purpose of the surveillance is to acquire foreign intelligence information, and the certification must set forth the basis for the certifying officials's belief that the information sought is the type of foreign intelligence information described"); *United States v. Pelton*, 835 F.2d 1067, 1075-76 (4th Cir. 1987)("We also reject Pelton's claim that the 1985 FISA surveillance was conducted primarily for the purpose of his criminal prosecution, and not primarily for the purpose of obtaining foreign intelligence information. . . . We agree with the district court that the primary purpose of the surveillance, both initially and throughout was to gather foreign intelligence information. It is clear that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used . . . as evidence in a criminal trial"); *United States v. Sarkissian*, 841 F.2d 959, 907-8 (9th Cir. 1988)("Defendants rely on the primary purpose test articulated in *United States v. Truong Dinh Hung*. . . . One other court has applied the primary purpose test. Another court has rejected it . .. distinguishing *Truong*. A third court has declined to decide the issue. We also decline to decide the issue"); *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991)("Appellants attack the government's surveillance on the ground that it was undertaken not for foreign intelligence purposes, but to gather evidence for a criminal prosecution. FISA applications must contain, among other things, a certification that the purpose of the requested surveillance is the gathering of foreign intelligence information. . . . Although the evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance").

[20] "Current law requires that FISA be used only where foreign intelligence gathering is the sole or primary purpose of the investigation. This section will clarify that the certification of a FISA request is supportable where foreign intelligence gathering is 'a' purpose of the investigation. This change would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts," *DoJ* at §153.

demanding standard than the "a purpose" threshold proposed by the Justice Department, but a clear departure from the original "the purpose" entry point. FISA once described a singular foreign intelligence focus prerequisite for any FISA surveillance application. Section 504 of the Act further encourages coordination between intelligence and law enforcement officials, and states that such coordination is no impediment to a "significant purpose" certification, 50 U.S.C. 1806(k), 1825(k).[21]

Protective Measures. The Act reenforces two kinds of safeguards, one set designed to prevent abuse and the other to protect those who assist the government. The sunset clause is perhaps the best known of the Act's safeguards. Under the direction of section 224, many of the law enforcement and foreign intelligence authorities granted by the Act expire as of December 31, 2005.[22] The Act also fills some of the gaps in earlier sanctions available for official, abusive invasions of privacy. Prior law made it a federal crime to violate Title III (wiretapping), chapter

---

[21] "(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. (2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105." FISA defines "foreign power" and "agent of a foreign power" broadly, *see* note 33, *infra*, quoting, 50 U.S.C. 1801.

[22] "(a) Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a)[sharing grand jury information], 203(c)[procedures for sharing grand jury information], 205 [FBI translators], 208 [seizure of stored voice-mail], 210[subpoenas for communications provider customer records], 211[access to cable company communication service records], 213[sneak and peek], 216[pen register and trap and trace device amendments], 221[trade sanctions], and 222[assistance to law enforcement], and the amendments made by those sections) shall cease to have effect on December 31, 2005.

"(b) With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect," section 224.

The sections which expire are: 201 and 202 (adding certain terrorism crimes to the predicate list for Title III), 293(b)(sharing Title III information with foreign intelligence officers), 204 (clarifying the foreign intelligence exception to the law enforcement pen register and trap and trace device provisions), 206 (roving foreign intelligence surveillance), 207 (duration of foreign intelligence surveillance orders and extensions), 209 (treatment of voice mail as e-mail rather than as telephone conversation), 212 (service provider disclosures in emergency cases), 214 (authority for pen registers and trap and trace devices in foreign intelligence cases), 215 (production of tangible items in foreign intelligence investigations), 217 (intercepting computer trespassers' communications), 218 (foreign intelligence surveillance when foreign intelligence gathering is "a significant" reason rather than "the" reason for the surveillance), 219 (nationwide terrorism search warrants), 220 (nationwide communication records and stored e-mail search warrants), 223 (civil liability and administrative discipline for violations of Title III, chapter 121, and certain foreign intelligence prohibitions), and 225 (immunity for foreign intelligence surveillance assistance).

121 (e-mail and communications records), or chapter 206 (pen registers and trap and trace devices).[23] Victims of offenses under Title III and chapter 121 (but not chapter 206) were entitled to damages (punitive damages in some cases) and reasonable attorneys' fees,[24] but could not recover against the United States.[25] Chapter 121 alone insisted upon an investigation into whether disciplinary action ought to be taken when federal officers or employees were found to have intentionally violated its proscriptions, 18 U.S.C. 2707.

The Act augments these sanctions by authorizing a claim against the United States for not less than $10,000 and costs for violations of Title III, chapter 121, or the Foreign Intelligence Surveillance Act (FISA), by federal officials, and emphasizing the prospect of administrative discipline for offending federal officials, section 223.

Finally, the Act instructs the Department of Justice's Inspector General to designate an official to receive and review complaints of civil liberties violations by DoJ officers and employees, section 1001.

The second category of protective measures applies to service providers and others who help authorities track and gather communications information. For example, section 815 immunizes service providers who in good faith preserve customer records at the government's request until a court order authorizing access can be obtained.[26] Another allows providers to disclose customer records to protect the provider's rights and property and to disclose stored customer communications and records in emergency circumstances, section 212. Under pre-existing law providers could disclose the content of stored communications but not customer records. The Justice Department recommended the changes in the interests of greater protection against cybercrimes committed by terrorists and others.[27] A third section,

---

[23] 18 U.S.C. 2511, 2701, and 3121 (2000 ed.), respectively.

[24] 18 U.S.C. 2520 and 2707 (2000 ed.).

[25] *Spock v. United States*, 464 F.Supp. 510, 514 n.2 (S.D.N.Y. 1978); *Asmar v. IRS*, 680 F.Supp. 248, 250 (E.D.Mich. 1987).

[26] Prior law already granted service providers immunity for disclosure of customer records in compliance with a court access order, 18 U.S.C. 2703(f).

[27] "Existing law contains no provision that allows providers of electronic communications service to disclose the communications (or records relating to such communications) of their customers or subscribers in emergencies that threaten death or serious bodily injury. This section amends 18 U.S.C. §2702 to authorize such disclosures if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

"Current law also contains an odd disconnect: a provider may disclose the *contents* of the customer's communications in order to protect its rights or property but the current statute does not expressly permit a provider to voluntarily disclose *non-content* records (such as a subscriber's login records). 18 U.S.C. 2702(b)(5). This problem substantially hinders the ability of providers to protect themselves from cyber-terrorists and criminals. Yet the right to disclose the contents of communications necessarily implies the less intrusive ability to disclose non-content records. In order to promote the protection of our nation's critical infrastructures, this section's amendments allow communications providers to voluntarily disclose both content and non-content records to protect their computer systems," *DoJ* at

section 222 promises reasonable compensation for service providers and anyone else who help law enforcement install or apply pen registers or trap and trace devices,[28] but makes it clear that nothing in the Act is intended to expand communications providers' obligation to make modifications in their systems in order to accommodate law enforcement needs.[29]

Foreign Intelligence Investigations

Although both criminal investigations and foreign intelligence investigations are conducted in the United States, criminal investigations seek information about unlawful activity; foreign intelligence investigations seek information about other countries and their citizens. Foreign intelligence is not limited to criminal, hostile, or even governmental activity. Simply being foreign is enough.[30]

Restrictions on intelligence gathering within the United States mirror American abhorrence of the creation of a secret police, coupled with memories of intelligence gathering practices during the Vietnam conflict which some felt threatened to chill robust public debate. Yet there is no absolute ban on foreign intelligence gathering in the United States. Congress enacted the Foreign Intelligence Surveillance Act (FISA),[31] something of a Title III for foreign intelligence wiretapping conducted in this country, after the Supreme Court made it clear that the President's authority to see to national security was insufficient to excuse warrantless wiretapping of suspected terrorists who had no identifiable foreign connections, *United States v. United States District Court*, 407 U.S. 297 (1972). FISA later grew to include procedures for physical searches in foreign intelligence cases, 50 U.S.C. 1821-1829, for pen register and trap and trace orders, 50 U.S.C. 1841-1846, and for access to records from businesses engaged in car rentals, motel accommodations, and storage

---

§110.

[28] Chapter 206 had long guaranteed providers and others reasonable compensation, 18 U.S.C. 3124(c), but section 216 of the Act expands the circumstances under which the authorities may request assistance including requests for the help of those not specifically mentioned in the court order. Section 222 makes it clear the expanded obligation to provide assistance is matched by a corresponding right to compensation.

[29] Thus in the name of assisting in the execution of Title III, chapter 121, or chapter 206 order, the courts may not cite the Act as the basis for an order compelling a service provider to make system modifications or provide any other technical assistance not already required under 18 U.S.C. 2518(4), 2706, or 3124(c), *see,* H.R.Rep.No. 107-236, at 62-3 (2001) (emphasis added) ("This Act is not intended to affect obligations under Communications Assistance for Law Enforcement Act [which addresses law enforcement-beneficial system modifications and the compensation to be paid for the changes], nor does the act impose any *additional* technical obligation or requirement on a provider of wire or electronic communication service or other person to furnish facilities or technical assistance").

[30] *E.g.*, As amended by section 902 of the Act, "'foreign intelligence' means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, *or international terrorist activities*," 50 U.S.C. 401a(2)(language added by the Act in italics).

[31] 50 U.S.C. 1801 *et seq.*

lockers, 50 U.S.C. 1861-1863 (2000 ed.). Intelligence authorities gained narrow passages through other privacy barriers as well.[32]

In many instances, access was limited to information related to the activities of foreign governments or their agents in this country, not simply relating to something foreign here. FISA, for example, is directed at foreign governments, international terrorists, and their agents, spies and saboteurs.[33] There were and still are extra

---

[32] *E.g.*, 18 U.S.C. 2709 (counterintelligence access to telephone toll and transaction records), 12 U.S.C. 3414 (right to financial privacy), 15 U.S.C. 1681u(fair credit reporting).

[33] "As used in this subchapter: (a) 'Foreign power' means – (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.

"(b) 'Agent of a foreign power' means – (1) any person other than a United States person, who – (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (2) any person who – (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

"(c) 'International terrorism' means activities that – (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended – (A) to intimidate or coerce ac ivilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnaping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

"(d) 'Sabotage' means activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States.

"(e) 'foreign intelligence information' means – (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an

safeguards if it appears that an intelligence investigation may generate information about Americans ("United States persons," *i.e.,* citizens or permanent resident aliens).[34] The procedures tend to operate under judicial supervision and tend to be confidential as a matter of law, prudence, and practice.

The Act eases some of the restrictions on foreign intelligence gathering within the United States, and affords the U.S. intelligence community greater access to information unearthed during a criminal investigation, but it also establishes and expands safeguards against official abuse. More specifically, it:

- permits "roving" surveillance (court orders omitting the identification of the particular instrument, facilities, or place where the surveillance is to occur when the court finds the target is likely to thwart identification with particularity)

- increases the number of judges on the FISA court from 7 to 11

- allows application for a FISA surveillance or search order when gathering foreign intelligence is *a significant* reason for the application rather than *the* reason

- authorizes pen register and trap & trace device orders for e-mail as well as telephone conversations

- sanctions court ordered access to any tangible item rather than only business records held by lodging, car rental, and locker rental businesses

- carries a sunset provision

- establishes a claim against the U.S. for certain communications privacy violations by government personnel

- expands the prohibition against FISA orders based solely on an American's exercise of his or her First Amendment rights.

---

agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to – (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States," 50 U.S.C. 1801.

[34] Strictly speaking for FISA purposes, a United States person "means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section," 50 U.S.C. 1801(i).

FISA. FISA is in essence a series of procedures available to secure court orders in certain foreign intelligence cases.[35] It operates through the judges of a special court which prior to the Act consisted of seven judges, scattered throughout the country, two of whom were from the Washington, D.C. area. The Act, in section 208, authorizes the appointment of four additional judges and requires that three members of the court reside within twenty miles of the District of Columbia, 50 U.S.C. 1803(a).

Search and Surveillance for Intelligence Purposes. Unless directed at a foreign power, the maximum duration for FISA surveillance orders and extensions was once ninety days and forty-five days for physical search orders and extensions, 50 U.S.C. 1805(e), 1824(d)(2000 ed.). The Act, in section 207, extends the maximum tenure of physical search orders to ninety days and in the case of both surveillance orders and physical search orders extends the maximum life of an order involving an agent of a foreign power to 120 days, with extensions for up to a year, 50 U.S.C. 1805(e), 1824(d). This represents a compromise over the Justice Department's original proposal which would have set the required expiration date for orders at one year instead of 120 days, *Draft* at §151.[36]

Section 901 of the Act address a concern raised during the 106th Congress relating to the availability of the FISA orders and the effective use of information gleaned from the execution of a FISA order.[37] It vests the Director of Central

---

[35] For a general discussion of FISA prior to enactment of the Act, *see*,Ba zan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance*, CRS REP.NO. RL30465 (Sept. 18, 2001).

[36] *See also, DoJ* at §151, "This section reforms a critical aspect of the Foreign Intelligence Surveillance Act (FISA). It will enable the Foreign Intelligence Surveillance Court (FISC), which presides over applications made by the U.S. government under FISA, to authorize the search and surveillance in the U.S. of officers and employees of foreign powers and foreign members of international terrorist groups for up to a year. Currently, the FISC may only authorize such searches and surveillance for up to 45 days and 90 days, respectively. The proposed change would bring the authorization period in line with that allowed for search and surveillance of the foreign establishments for which the foreign officers and employees work. The proposed change would have no effect on electronic surveillance of U.S. citizens or permanent resident aliens."

Section 314 of the Intelligence Authorization Act for Fiscal Year 2002 (Intelligence Authorization Act), P.L. 107-108, 115 Stat. 1394, 1402 (2001), further amended some of the time limits relating to FISA surveillance and physical searches, extending from 24 hours to 72 hours: (a) the time period during which agents might disseminate or use information secured pursuant to a FISA surveillance or search order but otherwise protected from dissemination or use by the order's minimization requirements; and (b) the permissible duration of emergency surveillance or searches after which surveillance or the search must stop or a FISA order application filed (50 U.S.C. 1801(h)(4), 1821(4)(D), 1805(f), 1824(e)).

[37] *See e.g.*, S.Rep.No. 106-352, at 3, 6, 7 (2000)("The Office of Intelligence Policy and Review (OIPR) in the Department of Justice is responsible for advising the Attorney General on matters relating to the national security of the United States. As part of its responsibilities, the OIPR prepares and presents to the Foreign Intelligence Surveillance Court (FISC) all applications for electronic surveillance and physical searches under the Foreign Intelligence Surveillance Act . . . . Agencies have informed the Committee that the FISA application

Intelligence with the responsibility to formulate requirements and priorities for the use of FISA to collect foreign intelligence information. He is also charged with the responsibility of assisting the Attorney General in the efficient and effective dissemination of FISA generated information (50 U.S.C. 403-3(c)).

Pen Registers and Trap and Trace Devices for Intelligence Gathering. Section 214 grants the request of the Department of Justice by dropping requirements which limited FISA pen register and trap and trace device orders to facilities used by foreign agents or those engaged in international terrorist or clandestine intelligence activities, 50 U.S.C. 1842(c)(3)(2000 ed.).[38] It is enough that the order is sought as part of an investigation to protect against international terrorism or clandestine intelligence activities and is not motivated solely by an American's exercise of his or her First Amendment rights. Elsewhere (section 505), the Act drops a similar limitation for intelligence officials' access to telephone records, 18 U.S.C.

---

process, as interpreted by the OIPR is administratively burdensome and, at times, extremely slow. Many applications undergo months of scrutiny before submission to the court because the OIPR prescribes standards and restrictions not imposed by the statute. . . . In particular, the OIPR has been criticized for an overly restrictive interpretation of the FISA 'currency' requirement. This is the issue of how recent a subject's activities must be to support a finding of probable cause that the subject is engaged in clandestine intelligence gathering activities. . . .While existing law does not specifically address ``past activities,'' it does not preclude, and legislative history supports, the conclusion that past activities may be part of the totality of circumstances considered by the FISC in making a probable cause determination. . . . By definition, information collected pursuant to a court order issued under the Foreign Intelligence Surveillance Act is foreign intelligence not law enforcement information. Accordingly, the Committee wants to clarify that the FISA `take' can and must be shared by the Federal Bureau of Investigation with appropriate intelligence agencies. For the intelligence mission of the United States to be successful, there must be a cooperative and concerted effort among intelligence agencies. Any information collected by one agency under foreign intelligence authorities that could assist another agency in executing its lawful mission should be shared fully and promptly. Only then can the United States Government pursue aggressively important national security targets including, for example, counterterrorist and counternarcotics targets"); *see also*, 147 *Cong.Rec.* S799-803 (daily ed. Feb. 24, 2000)(remarks of Sens. Specter, Torricelli and Biden).

[38] "When added to FISA two years ago, the pen register/trap and trace section was intended to mirror the criminal pen/trap authority defined in 18 U.S.C. §3123. The FISA authority differs from the criminal authority in that it requires, in addition to a showing of relevance, an additional factual showing that the communications device has been used to contact an 'agent of a foreign power' engaged in international terrorism or clandestine intelligence activities. This has the effect of making the FISA pen/trap authority much more difficult to obtain. In fact, the process of obtaining FISA pen/trap authority is only slightly less burdensome than the process for obtaining full electronic surveillance authority under FISA. This stands in stark contrast to the criminal pen/trap authority, which can be obtained quickly from a local court, on the basis of a certification that the information to be obtained is relevant to an ongoing investigation. The amendment simply eliminates the 'agent of a foreign power' prong from the predication, and thus makes the FISA authority more closely track the criminal authority," *DoJ* at §155.

2709(b), and under the Right to Financial Privacy Act, 12 U.S.C. 3414(a)(5)(A), as well as the Fair Credit Reporting Act, 15 U.S.C. 1681u.[39]

Section 214 adjusts the language of the FISA pen register-trap and trace authority to permit its use to capture source and destination information relating to electronic communications (*e.g.*, e-mail) as well as telephone communications, 50 U.S.C. 1842(d). The section makes it clear that requests for a FISA pen register-trap and trace order, like requests for other FISA orders, directed against Americans (U.S. persons) may not be based solely on activities protected by the First Amendment, 50 U.S.C. 1842, 1843.

Third Party Cooperation and Tangible Evidence. As in the case of criminal investigations, the Act has several sections designed to encourage third party cooperation and to immunize third parties from civil liability for their assistance. FISA orders may include instructions directing specifically identified third parties to assist in the execution of the order, 50 U.S.C. 1805(c)(2)(B). The Act permits inclusion of a general directive for assistance when the target's activities are designed to prevent more specific identification, section 206, and immunizes in 50 U.S.C. 1805(h), those who provide such assistance, section 225.[40]

---

[39] Except in the case of certain credit information, these are not court procedures, but written requests for third party records which would otherwise to be entitled to confidentiality. Section 505, in response to the Justice Department's suggestion, allows FBI field offices to make the requests, *see DoJ* at §157 ("At the present time, National Security Letter (NSL) authority exists in three separate statutes: the Electronic Communications Privacy Act (for telephone and electronic communications records), the Financial Right to Privacy Act (for financial records), and the Fair Credit Reporting Act (for credit records). Like the FISA pen register/trap and trace authority described above, NSL authority requires both a showing of relevance and a showing of links to an 'agent of a foreign power.' In this respect, they are substantially more demanding than the analogous criminal authorities, which require only a certification of relevance. Because the NSLs require documentation of the facts supporting the 'agent of a foreign power' predicate and because they require the signature of a high-ranking official at FBI headquarters, they often take months to be issued. This is in stark contrast to criminal subpoenas, which can be used to obtain the same information, and are issued rapidly at the local level. In many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from headquarters, and served. The section would streamline the process of obtaining NSL authority, and also clarify the FISA Court can issue orders compelling production of consumer reports").

[40] When it requested the amendment, the Department of Justice explained that the "provision expands the obligations of third parties to furnish assistance to the government under FISA. Under current FISA provisions, the government can seek information and assistance from common carriers, landlords, custodians and other persons specified in court-ordered surveillance. Section 152 would amend FISA to expand existing authority to allow, 'in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person that a common carrier, landlord, custodian or other persons not specified in the Court's order be required to furnish the applicant information and technical assistance necessary to accomplish electronic surveillance in a manner that will protect its secrecy and produce a minimum of interference with the services that such person is providing to the target of electronic surveillance.' This would enhance the FBI's ability to monitor international terrorists and intelligence officers who are

Prior to the Act, FISA allowed federal intelligence officers to seek a court order for access to certain car rental, storage, and hotel accommodation records, 50 U.S.C. 1861 to 1863 (2000 ed.). The Justice Department asked that the authority be replaced with permission to issue administrative subpoenas for any tangible item regardless of the business (if any) of the custodian.[41] The Act amends the provisions, preserving the court order requirement. Yet it allows the procedure to be used in foreign intelligence investigations, conducted to protect against international terrorism or clandestine intelligence activities,[42] in order to seize any tangible item regardless of who is in possession of the item, and continues in place the immunity for good faith compliance by third party custodians, section 215.

In a related provision, Section 358 amends the –

- purposes section of the Currency and Foreign Transaction Reporting Act (31 U.S.C. 5311);
- •s uspicious activities reporting requirements section of that Act (31 U.S.C. 5318(g)(4)(B);
- availability of records section of that Act (31 U.S.C. 5319);
- purposes section of the Bank Secrecy Act (12 U.S.C. 1829b(a);
- the Secretary of the Treasury's authority over uninsured banks and other financial institutions under that Act (12 U.S.C. 1953(a);
- access provisions of the Right to Financial Privacy Act (12 U.S.C. 3412(2)(a), 3414(a)(1), 3420(a)(2); and
- access provisions of the Fair Credit Reporting Act (15 U.S.C. 1681u, 1681v;

---

trained to thwart surveillance by rapidly changing hotel accommodations, cell phones, Internet accounts, etc., just prior to important meetings or communications. Under the current law, the government would have to return to the FISA Court for an order that named the new carrier, landlord, etc., before effecting surveillance. Under the proposed amendment, the FBI could simply present the newly discovered carrier, landlord, custodian or other person with a generic order issued by the Court and could then effect FISA coverage as soon as technically feasible," *DoJ* at 152.

Section 314 of the Intelligence Authorization Act immunizes those who assist in the execution of either a FISA surveillance or physical search order (50 U.S.C. 1805(i)), 115 Stat. 1402.

[41] "The 'business records' section of FISA (50 U.S.C. §§ 1861 and 1862) requires a formal pleading to the Court and the signature of a FISA judge (or magistrate). In practice, this makes the authority unavailable for most investigative contexts. The time and difficulty involved in getting such pleadings before the Court usually outweighs the importance of the business records sought. Since its enactment, the authority has been sought less than five times. This section would delete the old authority and replace it with a general 'administrative subpoena' authority for documents and records. This authority, modeled on the administrative subpoena authority available to drug investigators pursuant to Title 21, allows the Attorney General to compel production of such records upon a finding that the information is relevant," *DoJ* at §156.

[42] Section 314 of the Intelligence Authorization Act further amended the section to permit orders relating to investigations "to obtain foreign intelligence information not concerning a United States person" in addition to those conducted to protect against terrorism and clandestine activities, 50 U.S.C. 1861(a)(1).

to clarify and authorize access of federal intelligence authorities to the reports and information gathered and protected under those Acts.[43]

Access to Law Enforcement Information. Shortly after September 11, sources within both Congress and the Administration stressed the need for law enforcement and intelligence agencies to more effectively share information about terrorists and their activities. On September 14, the Senate Select Committee on Intelligence observed that, "effective sharing of information between and among the various components of the government-wide effort to combat terrorists is also essential, and is presently hindered by cultural, bureaucratic, resource, training and, in some cases, legal obstacles," H.R.Rep.No. 107-63, at 10 (2001). The Justice Department's consultation draft of September 20 offered three sections which would have greatly expanded the intelligence community's access to information collected as part of a criminal investigation. First, it suggested that information generated through the execution of a Title III order might be shared in connection with the duties of any executive branch official, *Draft* at §103.[44]

---

[43] H.R.Rep.No. 107-205, at 60-1 (2001)("This section clarifies the authority of the Secretary of the Treasury to share Bank Secrecy Act information with the intelligence community for intelligence or counterintelligence activities related to domestic or international terrorism. Under current law, the Secretary may share BSA information with the intelligence community for the purpose of investigating and prosecuting terrorism. This section would make clear that the intelligence community may use this information for purposes unrelated to law enforcement.

"The provision would also expand a Right to Financial Privacy Act (RFPA) exemption, currently applicable to law enforcement inquiries, to allow an agency or department to share relevant financial records with another agency or department involved in intelligence or counterintelligence activities, investigations, or analyses related to domestic or international terrorism. The section would also exempt from most provisions of the RFPA a government authority engaged in investigations of or analyses related to domestic or international terrorism. This section would also authorize the sharing of financial records obtained through a Federal grand jury subpoena when relevant to intelligence or counterintelligence activities, investigations, or analyses related to domestic or international terrorism. In each case, the transferring governmental entity must certify that there is reason to believe that the financial records are relevant to such an activity, investigation, or analysis.

"Finally, this section facilitates government access to information contained in suspected terrorists' credit reports when the governmental inquiry relates to an investigation of, or intelligence activity or analysis relating to, domestic or international terrorism. Even though private entities such as lenders and insurers can access an individual's credit history, the government is strictly limited in its ability under current law to obtain the information. This section would permit those investigating suspected terrorists prompt access to credit histories that may reveal key information about the terrorist's plan or source of funding--without notifying the target. To obtain the information, the governmental authority must certify to the credit bureau that the information is necessary to conduct a terrorism investigation or analysis. The amendment would also create a safe harbor from liability for credit bureaus acting in good faith that comply with a government agency's request for information").

[44] *See also, DoJ* at §103, "This section facilities the disclosure of Title III information to other components of the intelligence community in terrorism investigations. At present, 18 U.S.C. §2517(1) generally allows information obtained via wiretap to be disclosed only to the extent that it will assist a criminal investigation. One must obtain a court order to disclose Title III information in non-criminal proceedings. Section 109 [103] would modify the

Second, it recommended a change in Rule 6(e) of the Federal Rules of Criminal Procedure that would allow disclosure of grand jury material to intelligence officials, *Draft* at §354.[45]

Third, it proposed elimination of all constraints on sharing foreign intelligence information uncovered during a law enforcement investigation, mentioning by name the constraints in Rule 6(e) and Title III, *Draft* at §154.[46]

The Act combines versions of all three in section 203. Perhaps because of the nature of the federal grand jury, resolution of the grand jury provision proved especially difficult. The federal grand jury is an exceptional institution. Its purpose is to determine if a crime has been committed, and if so by whom; to indict the guilty; and to refuse to indict the innocent. Its probes may begin without probable cause or any other threshold of suspicion.[47] It examines witnesses and evidence ordinarily secured in its name and questioned before it by Justice Department prosecutors. Its

---

wiretap statutes to permit the disclosure of Title III-generated information to a non-law enforcement officer for such purposes as furthering an intelligence investigation. This will harmonize Title III standards with those of the Foreign Intelligence Surveillance Act (FISA), which allows such information-sharing. Allowing disclosure under Title III is particularly appropriate given that the requirements for obtaining a Title III surveillance order in general are more stringent than for a FISA order, and because the attendant privacy concerns in either situation are similar and are adequately protected by existing statutory provisions."

[45] *See also, DoJ* at §354, "This section makes changes in Rule 6(e) of the Federal Rules of Criminal Procedure, relating to grand jury secrecy, to facilitate the sharing of information with federal law enforcement, intelligence, protective, national defense, and immigration personnel in terrorism and national security cases. The section is in part complimentary to section 154 of the bill, relating to sharing of foreign intelligence information, and reflects a similar purpose of promoting a coordinated governmental response to terrorist and national security threats." Contrary to the implication here section 154 deals with sharing information gathered by law enforcement officials not with information gathered by intelligence officers

[46] *See also, DoJ* at §154, "This section provides that foreign intelligence information obtained in criminal investigations, including grand jury and electronic surveillance information, may be shared with other federal government personnel having responsibilities relating to the defense of the nation and its interests. With limited exceptions, it is presently impossible for criminal investigators to share information obtained through a grand jury (including through the use of grand jury subpoenas) and information obtained from electronic surveillance authorized under Title III with the intelligence community. This limitation will be very significant in some criminal investigations. For example, grand jury subpoenas often are used to obtain telephone, computer, financial and other business records in organized crime investigations. Thus, these relatively basic investigative materials are inaccessible for examination by intelligence community analysts working on related transnational organized crime groups. A similar problem occurs in computer intrusion investigations: grand jury subpoenas and Title III intercepts are used to collect transactional data and to monitor the unknown intruders. The intelligence community will have an equal interest in such information, because the intruder may be acting on behalf of a foreign power."

[47] *Blair v. United States*, 250 U.S. 273, 281 (1919)(the grand jury "is a grand inquest, a body with powers of investigation and inquisition, the scope of whose inquiries is not to be limited narrowly by questions of propriety or forecasts of whether any particular individual will be found properly subject to an accusation of crime").

affairs are conducted in private and outside the presence of the court. Only the attorney for the government, witnesses under examination, and a court reporter may attend its proceedings, F.R.Crim.P. 6(d). Matters occurring before the grand jury are secret and may be disclosed by the attending attorney for the government and those assisting the grand jury only in the performance of their duties; in presentation to a successor grand jury; or under court order for judicial proceedings, for inquiry into misconduct before the grand jury, or for state criminal proceedings, F.R.Crim.P. 6(e).

The Act, in section 203(a), allows disclosure of matters occurring before the grand jury to "any federal law enforcement, intelligence, protective, immigration, national defense, or national security" officer to assist in the performance of his official duties, F.R.Crim.P. 6(e)(3)(C)(i)(V).[48]

Critics may protest that the change could lead to the use of the grand jury for intelligence gathering purposes, or less euphemistically, to spy on Americans.[49] The proposal was never among those scheduled to sunset, but earlier versions of the section followed the path used for most other disclosures of grand jury material: prior

---

[48] These officers may receive: (1) "foreign intelligence information" that is, information regardless whether it involves Americans or foreign nationals that "[a] relates to the ability of the United States to protect against – (aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; (cc) clandestine intelligence activities by an intelligence service or network of a foreign power;" or [b] "with respect to a foreign power or foreign territory that relates to – (aa) the national defense or security of the United States; or (bb) the conduct of the foreign affairs of the United States," F.R.Crim.P. 6(e)(3)(C)(iv); (2) when the matters involve foreign intelligence or counterintelligence, that is, [a] "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" or [b] "information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, *or international terrorist activities*," 50 U.S.C. 401a(2),(3)(language added by section 902 of the Act in italics).

[49] Beale & Felman, *The Consequences of Enlisting Federal Grand Juries in the War on Terrorism: Assessing the USA PATRIOT Act's Changes to Grand Jury Secrecy*, 25 HARVARD JOURNAL OF LAW & PUBLIC POLICY 699, 719-20 (2002)("There is a significant danger that the rule permitting disclosure will be treated as the de facto authorization of an expansion of the grand jury's investigative role to encompass seeking material relevant only to matters of national security, national defense, immigration, and so forth. The grand jury's awesome powers should not be unwittingly extended to a much wider range of issues. . . Since the grand jury operates in secret, there are no public checks on the scope of its investigations, and witnesses are not permitted to challenge its jurisdiction. Only the supervising court is in a position to keep the grand jury's investigation within proper bounds. Requiring judicial approval of foreign intelligence and counterintelligence information disclosures would provide a natural check against the temptation to manipulate the grand jury to develop information for unauthorized purposes"); *but see*, Scheidegger et al., *Federalist Society White Paper on The USA PATRIOT Act of 2001: Criminal Procedure Sections* 6 (Nov. 2001)("The grand jury secrecy rule is a rule of policy which has always had exceptions, and it has been frequently modified. The secrecy rule has no credible claim to constitutional stature").

court approval, H.R.Rep.No. 107- 236, at 73 (2001). The Act, in section 203(a), instead calls for confidential notification of the court that a disclosure has occurred and the entity to whom it was made, F.R.Crim.P. 6(e)(3)(C)(iii). It also insists that the Attorney General establish implementing procedures for instances when the disclosure "identifies" Americans (U.S. persons), section 203(c).

Law enforcement officials may share Title III information with the intelligence community under the same conditions, section 203(b),[50] although the grand jury and Title III sharing provisions differ in at least three important respects. The court need not be notified of Title III disclosures. On the other hand, the authority for sharing Title III information expires on December 31, 2005, section 224, and agencies and their personnel guilty of intentional improper disclosures may be subject to a claim for damages and disciplinary action, 18 U.S.C. 2520.

The third subsection of section 203 remains something of an enigma. It speaks in much the same language as its counterparts. It allows law enforcement officials to share information with the intelligence community, "notwithstanding any other provisions of law," section 203(d).[51] It either swallows the other subsections, or supplements them. Several factors argue for its classification as a supplement. Congress is unlikely to have crafted subsections (a), (b) and (c) only to completely

---

[50] Information derived from a Title III interception may be shared with any other federal law enforcement, intelligence, protective, immigration, national defense, or national security officer if it regards: (1) "foreign intelligence information" that is, information irrespective of whether it involves Americans or foreign nationals that "[A] relates to the ability of the United States to protect against – (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; (iii) clandestine intelligence activities by an intelligence service or network of a foreign power;" or [B] "with respect to a foreign power or foreign territory that relates to – (i) the national defense or security of the United States; or (ii) the conduct of the foreign affairs of the United States;" (2) when the matters involve foreign intelligence or counterintelligence as defined by 50 U.S.C. 401a (as amended by section 902 of the Act), *i.e.*, "As used in this Act: (1) The term 'intelligence' includes foreign intelligence and counterintelligence. (2) The term 'foreign intelligence' means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, *or international terrorist activities*. (3) The term 'counterintelligence' means information gathered and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" (language added by section 902 in italics).

[51] "Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C.) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information," §203(d)(1). The subsection goes to define "foreign intelligence information" in the same terms used to define that phrase in Title III (18 U.S.C. 2510(19)) and in Rule 6(e)(F.R.Crim.P.6(e)(3)(C)(iv)), §203(d)(2).

nullify them in subsection (d). Without a clear indication to the contrary, the courts are unlikely to find that Congress intended nullification.[52] By gathering the three into a single section Congress avoided the suggestion that the phrase "notwithstanding any other provision of law" constitutes surplusage. The Title III and grand jury sharing procedures are not in other provisions of law, they are now subsections of the same provision of law. Moreover, Congress seemed to signal an intent for the subsections to operate in tandem when it dropped the language of the original Justice Department proposal which expressly identified Title III and Rule 6(e) as examples of the restrictions to be overcome by the universal sharing language.[53]

Section 203 deals with earlier legal impediments to sharing foreign intelligence information unearthed during the course of a criminal investigation. Section 905 looks to dissolve the barriers may be more cultural than legal. Under it, the Attorney General is to issue guidelines governing the transmittal to the Director of Central Intelligence of foreign intelligence information that surfaces in the course of a criminal investigation. The section also instructs the Attorney General to promulgate guidelines covering reports to the Director of Central Intelligence on whether a criminal investigation has been initiated or declined based on an intelligence community referral, 50 U.S.C. 403-5b. To ensure effective use of increased information sharing, section 908 calls for training of federal, state and local officials to enable them to recognize foreign intelligence information which they encounter in their work and how to use it in the performance of their duties, 28 U.S.C. 509 note.

Increasing Institutional Capacity. As noted elsewhere, the Act liberalizes authority for the FBI to hire translators, section 203, which enhances its capacity to conduct both criminal and foreign intelligence investigations. The Act also reflects sentiments expressed earlier concerning coordinated efforts to develop a

---

[52] *Duncan v. Walker*, 121 S.Ct. 2120, 2125 (2001)(internal quotation marks and parallel citations omitted)("It is our duty to give effect, if possible, to every clause and word of a statute. *United States v. Menasche*, 348 U.S. 528, 538-539 (1955) (quoting *Montclair v. Ramsdell,* 107 U.S. 147, 152 (1883)); see also *Williams v. Taylor,* 529 U.S. 362, 404 (2000) (describing this rule as a cardinal principle of statutory construction); *Market Co. v. Hoffman,* 101 U.S. 112, 115 (1879)(As early as in Bacon's Abridgment, sect. 2, it was said that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant). We are thus reluctant to treat statutory terms as surplusage in any setting. *Babbitt v. Sweet Home Chapter, Communities for Great Ore.,* 515 U.S. 687, 698 (1995); see also *Ratzlaf v. United States,* 510 U.S. 135, 140 (1994)").

It is not possible to conclude that Congress intended the universal subsection (d) to apply until sunset and the grand jury and Title III subsections (a), (b), and (c) to operate thereafter, because the Title III subsection expires at the same time as the universal subsection.

[53] *Draft* at §154, "Notwithstanding any other provision of law, it shall be lawful for foreign intelligence information obtained as part of ac riminal investigation (including, without limitation, information subject to Rule 6(e) of the Federal Rules of Criminal Procedure and information obtained pursuant to chapter 119 of title 18, United States Code [*i.e.* Title III]) to be provided to any federal law enforcement, intelligence, protective, or national defense personnel, or any federal personnel responsible for administering the immigration laws of the United States, or to the President and the Vice President of the United States."

computerized translation capability to be used in foreign intelligence gathering.[54] Section 907 instructs the Director of the Central Intelligence, in consultation with the Director of the FBI, to report on the creation of a National Virtual Translation Center. The report is to include information concerning staffing, allocation of resources, compatibility with comparable systems to be used for law enforcement purposes, and features which permit its efficient and secure use by all of the intelligence agencies.

Money Laundering

In federal law, money laundering is the flow of cash or other valuables derived from, or intended to facilitate, the commission of a criminal offense. It is the movement of the fruits and instruments of crime. Federal authorities attack money laundering through regulations, international cooperation, criminal sanctions, and forfeiture.[55] The Act bolsters federal efforts in each area.

Regulation. Prior to passage of the Act, the Treasury Department already enjoyed considerable authority to impose reporting and record-keeping standards on financial institutions generally and with respect to anti-money laundering matters in particular.[56]

---

[54] "The Committee is concerned that intelligence in general, and intelligence related to terrorism in particular, is increasingly reliant on the ability of the Intelligence Community to quickly, accurately and efficiently translate information in a large number of languages. Many of the languages for which translation capabilities are limited within the United States Government are the languages that are of critical importance in our counterterrorism efforts. The Committee believes that this problem can be alleviated by applying cutting-edge, internet-like technology to create a 'National Virtual Translation Center.' Such a center would link secure locations maintained by the Intelligence Community throughout the country and would apply digital technology to network, store, retrieve, and catalogue the audio and textual information. Foreign intelligence could be collected technically in one location, translated in a second location, and provided to an Intelligence Community analyst in a third location.

"The Committee notes that the CIA, FBI NSA and other intelligence agencies have applied new technology to this problem. The Committee believes that these efforts should be coordinated so that the solution can be applied on a Community-wide basis. Accordingly, the Committee directs the Director of Central Intelligence, in consultation with the Director of the FBI, and other heads of departments and agencies within the Intelligence Community, to prepare and submit to the intelligence committees by June 1, 2002, a report concerning the feasibility and structure of a National Virtual Translation Center, including recommendations regarding the establishment of such a center and the funding necessary to do so," S.Rep.No. 107-63, at 11 (2001).

[55] For a brief overview, *see*, Murphy, *Money Laundering: Current Law and Proposals*, CRS REP.NO. RS21032 (DEC. 21, 2001).

[56] *See e.g.*, 12 U.S.C. 1829b (retention or records by insured depository institutions), 1951-1959 (record-keeping by financial institutions); 31 U.S.C. 5311 ("It is the purpose of this subchapter [31 U.S.C. 5311 et seq.] (except section 5315 [relating to foreign current transaction reports]) to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings").

Records and Reports. For instance, under the Currency and Financial Transaction Reporting Act, a component of the Bank Secrecy Act, anyone who transports more than $10,000 into or out of the United States must report that fact to the Treasury Department, 31 U.S.C. 5316. Banks, credit unions, and certain other financial institutions must likewise report identifying information relating to cash transactions in excess of $10,000 to the Treasury Department (CTRs), 31 U.S.C. 5313, 31 C.F.R. §103.22. Other businesses are required to report to the Internal Revenue Service the particulars relating to any transaction involving more than $10,000 in cash, 26 U.S.C. 6050I. Banks must file suspicious activity reports (SARs) with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) for any transactions involving more than $5,000 which they suspect may be derived from illegal activity, 31 U.S.C. 5318(g), 31 C.F.R. §103.18. Money transmission businesses and those that deal in traveler's checks or money orders are under a similar obligation for suspicious activities involving more than $2,000, 31 U.S.C. 5318(g), 31 C.F.R. §103.18.

Among other things, the Act expands the authority of the Secretary of the Treasury over these reporting requirements. He is to promulgate regulations, pursuant to sections 356 and 321, under which securities brokers and dealers as well as commodity merchants, advisors and pool operators must file suspicious activity reports, 31 U.S.C. 5318 note; 31 U.S.C. 5312(2)(c)(1). Businesses which were only to report cash transactions involving more than $10,000 to the IRS are now required to files SARs as well,[57] reflecting Congress' view that the information provided the IRS may be valuable for other law enforcement purposes.[58] This concern is likewise

---

[57] Section 365, 31 U.S.C. 5331; Sec. 321, 31 U.S.C. 5312.

[58] H.R.Rep.No. 107-250, at 38-9 (2001)("Most importantly, the Committee found significant shortcomings in the use of information already in possession of the government. Section 6050I of the Internal Revenue Code requires that any person engaged in a trade or business (other than financial institutions required to report under the Bank Secrecy Act) file a report with the Federal government on cash transactions in excess of $10,000. Reports filed pursuant to this requirement provide law enforcement authorities with a paper trail that can, among other things, lead to the detection and prosecution of money laundering activity.

"Under current law, non-financial institutions are required to report cash transactions exceeding $10,000 to the Internal Revenue Service (IRS) on IRS Form 8300. Because the requirement that such reports be filed is contained in the Internal Revenue Code, Form 8300 information is considered tax return information, and is subject to the procedural and record-keeping requirements of section 6103 of the Internal Revenue Code. For example, section 6103(p)(4)(E) requires agencies seeking Form 8300 information to file a report with the Secretary of the Treasury that describes the procedures established and utilized by the agency for ensuring the confidentiality of the information. IRS requires that agencies requesting Form 8300 information file a 'Safeguard Procedures Report' which must be approved by the IRS before any such information can be released. For that reason, Federal, State and local law enforcement agencies are not given access to the Form 8300s as Congress anticipated when it last amended this statute. See 26 U.S.C. 6103(l)(15).

"While the IRS uses Form 8300 to identify individuals who may be engaged in tax evasion, Form 8300 information can also be instrumental in helping law enforcement authorities trace cash payments by drug traffickers and other criminals for luxury cars, jewelry, and other expensive merchandise. Because of the restrictions on their dissemination outlined above, however, Form 8300s are not nearly as accessible to law enforcement

reflected in section 357 which asks the Secretary of the Treasury to report on the Internal Revenue Service's role in the administration of the Currency and Foreign Transaction Reporting Act (31 U.S.C. 5311 et seq.), and what transfers of authority, if any, are appropriate.

Sections 351 and 355 address the liability for disclosure of suspicious activity reports (SARs). Prior to the Act, federal law prohibited financial institutions and their officers and employees from tipping off any of the participants in a suspicious transaction, 31 U.S.C. 5318(g)(2)(2000 ed.). Federal law, however, immunized the institutions and their officers and employees from liability for filing the reports and for failing to disclose that they had done so, 31 U.S.C. 5318(g)(3)(2000 ed.). Section 351 makes changes in both the immunity and the proscription. It adds government officials who have access to the reports to the anti-tip ban, *31 U.S.C. 5318*(g)*(2)*(A). It allows, but does not require, institutions to reveal SAR information in the context of employment references to other financial institutions, 31 U.S.C. 5318(g)(2)(B). Finally, it makes clear that the immunity does not extend to immunity from governmental action.[59] Section 355 expands the immunity to cover disclosures in

---

authorities as the various reports mandated by the Bank Secrecy Act, which can typically be retrieved electronically from a database maintained by the Treasury Department. The differential access to the two kinds of reports is made anomalous by the fact that Form 8300 elicits much the same information that is required to be disclosed by the Bank Secrecy Act. For example, just as Form 8300 seeks the name, address, and social security number of a customer who engages in a cash transaction exceeding $10,000 with a trade or business, Currency Transaction Reports (CTRs) mandated by the Bank Secrecy Act require the same information to be reported on a cash transaction exceeding $10,000 between a financial institution and its customer").

[59] "Subsection (a) of section [351] makes certain technical and clarifying amendments to 31 U.S.C. 5318(g)(3), the Bank Secrecy Act's 'safe harbor' provision that protects financial institutions that disclose possible violations of law or regulation from civil liability for reporting their suspicions and for not alerting those identified in the reports. The safe harbor is directed at Suspicious Activity Reports and similar reports to the government and regulatory authorities under the Bank Secrecy Act.

"First, section [351](a) amends section 5318(g)(3) to make clear that the safe harbor from civil liability applies in arbitration, as well as judicial, proceedings. Second, it amends section 5318(g)(3) to clarify the safe harbor's coverage of voluntary disclosures (that is, those not covered by the SAR regulatory reporting requirement). The language in section 5318(g)(3)(A) providing that 'any financial institution that * * * makes a disclosure pursuant to * * * any other authority * * * shall not be liable to any person' is not intended to avoid the application of the reporting and disclosure provisions of the Federal securities laws to any person, or to insulate any issuers from private rights of actions for disclosures made under the Federal securities laws.

"Subsection [351](b) amends section 5318(g)(2) of title 31--which currently prohibits notification of any person involved in a transaction reported in a SAR that a SAR has been filed--to clarify (1) that any government officer or employee who learns that a SAR has been filed may not disclose that fact to any person identified in the SAR, except as necessary to fulfill the officer or employee's official duties, and (2) that disclosure by a financial institution of potential wrongdoing in a written employment reference provided in response to a request from another financial institution pursuant to section 18(v) of the Federal Deposit Insurance Act, or in a written termination notice or employment reference provided in accordance with the rules of a securities self-regulatory organization, is not prohibited simply because the

employment references to other insured depository financial institutions provided disclosure is not done with malicious intent.[60]

The Financial Crimes Enforcement Network (FinCEN), a component within the Treasury Department long responsible for these anti-money laundering reporting and record-keeping requirements, 31 C.F.R. pt. 103, was administratively created in 1990 to provide other government agencies with an "intelligence and analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes," 55 *Fed.Reg.* 18433 (May 2, 1990).

The Act, in section 361, makes FinCEN a creature of statute, a bureau within the Treasury Department, 31 U.S.C. 310. Section 362 charges it with the responsibility of establishing a highly secure network to allow financial institutions to file required reports electronically and to permit FinCEN to provide those institutions with alerts and other information concerning money laundering protective measures, 31 U.S.C. 310 note.

Special Measures. In extraordinary circumstances involving international financial matters, the Act grants the Secretary of the Treasury, in consultation with other appropriate regulatory authorities, the power to issue regulations and orders involving additional required "special measures" and additional "due diligence" requirements to combat money laundering. The special measure authority, available under section 311, comes to life with the determination that particular institutions, jurisdictions, types of accounts, or types of transactions pose a primary money

---

potential wrongdoing was also reported in a SAR," H.R.Rep.No. 107-250, at 66 (2001).

[60] 31 U.S.C. 1828(w). "This section deals with the same employment reference issue addressed in section [351] but with respect to title 12. Occasionally banks develop suspicions that a bank officer or employee has engaged in potentially unlawful activity. These suspicions typically result in the bank filing a SAR. Under present law, however, the ability of banks to share these suspicions in written employment references with other banks when such an officer or employee seeks new employment is unclear. Section 208 would amend 12 U.S.C. 1828 to permit a bank, upon request by another bank, to share information in a written employment reference concerning the possible involvement of a current or former officer or employee in potentially unlawful activity without fear of civil liability for sharing the information, but only to the extent that the disclosure does not contain information which the bank knows to be false, and the bank has not acted with malice or with reckless disregard for the truth in making the disclosure," H.R.Rep.No. 107-250, at 67 (2001).

laundering concern.[61] These special measures may require U.S. financial institutions to:

- maintain more extensive records and submit additional reports relating to participants in foreign financial transactions with which they are involved
- secure beneficial ownership information with respect to accounts maintained for foreign customers
- adhere to "know-your-customer" requirements concerning foreign customers who use "payable-through accounts" held by the U.S. entity for foreign financial institutions
- keep identification records on foreign financial institutions' customers whose transactions are routed through the foreign financial institution's correspondent accounts with the U.S. financial institution
- honor limitations on correspondent or payable-through accounts maintained for foreign financial institutions.[62]

---

[61] 31 U.S.C. 5318A. The circumstances considered in the case of a suspect jurisdiction are: evidence of organized crime or terrorist transactions there; the extent to which the jurisdiction's bank secrecy or other regulatory practices encourage foreign use; the extent and effectiveness of the jurisdiction's banking regulation; the volume of financial transactions in relation to the size of the jurisdiction's economy; whether international watch dog groups (such as the Financial Action Task Force) have identified the jurisdiction as an offshore banking or secrecy haven; the existence or absence of a mutual legal assistance treaty between the U.S. and the jurisdiction; and the extent of official corruption within the jurisdiction. The institutional circumstances weighed before imposing special measures with respect to particular institutions or types of accounts or transactions include the intent to which the suspect institution or types of accounts or transactions are particularly attractive to money launderers, the extent to which they can be used by legitimate businesses, and the extent to which focused measures are likely to be successful.

[62] The House report describes these measures in greater detail: "Section [311] adds a new section 5318A to the Bank Secrecy Act, authorizing the Secretary of the Treasury to require domestic financial institutions and agencies to take one or more of five 'special measures' if the Secretary finds that reasonable grounds exist to conclude that a foreign jurisdiction, a financial institution operating outside the United States, a class of international transactions, or one or more types of accounts is a 'primary money laundering concern.' Prior to invoking any of the special measures contained in section 5318A(b), the Secretary is required to consult with the Chairman of the Board of Governors of the Federal Reserve System, any other appropriate Federal banking agency, the Securities and Exchange Commission, the National Credit Union Administration Board, and, in the sole discretion of the Secretary, such other agencies and interested parties as the Secretary may find to be appropriate. Among other things, this consultation is designed to ensure that the Secretary possesses information on the effect that any particular special measure may have on the domestic and international banking system. In addition, the Committee encourages the Secretary to consult with non-governmental 'interested parties,' including, for example, the Bank Secrecy Act Advisory Group, to obtain input from those who may be subject to a regulation or order under this section.

"Prior to invoking any of the special measures contained in section 5318A, the Secretary must consider three discrete factors, namely (1) whether other countries or multilateral groups have taken similar action; (2) whether the imposition of the measure would create a significant competitive disadvantage, including any significant cost or burden associated with compliance, for firms organized or licensed in the United States; and (3) the extent to which the action would have an adverse systemic impact on the payment system or legitimate

business transactions.

"Finally, subsection (a) makes clear that this new authority is not to be construed as superseding or restricting any other authority of the Secretary or any other agency.

"Subsection (b) of the new section 5318A outlines the five 'special measures' the Secretary may invoke against a foreign jurisdiction, financial institution operating outside the U.S., class of transaction within, or involving, a jurisdiction outside the U.S., or one or more types of accounts, that he finds to be of primary money laundering concern.

"The first such measure would require domestic financial institutions to maintain records and/or file reports on certain transactions involving the primary money laundering concern, to include any information the Secretary requires, such as the identity and address of participants in a transaction, the legal capacity in which the participant is acting, the beneficial ownership of the funds (in accordance with steps that the Secretary determines to be reasonable and practicable to obtain such information), and a description of the transaction. The records and/or reports authorized by this section must involve transactions from a foreign jurisdiction, a financial institution operating outside the United States, or class of international transactions within, or involving, a foreign jurisdiction, and are not to include transactions that both originate and terminate in, and only involve, domestic financial institutions.

"The second special measure would require domestic financial institutions to take such steps as the Secretary determines to be reasonable and practicable to ascertain beneficial ownership of accounts opened or maintained in the U.S. by a foreign person (excluding publicly traded foreign corporations) associated with what has been determined to be a primary money laundering concern.

"The third special measure the Secretary could impose in the case of a primary money laundering concern would require domestic financial institutions, as a condition of opening or maintaining a 'payable-through account' for a foreign financial institution, to identify each customer (and representative of the customer) who is permitted to use or whose transactions flow through such an account, and to obtain for each customer (and representative) information that is substantially comparable to the information it would obtain with respect to its own customers. A 'payable-through account' is defined for purposes of the legislation as an account, including a transaction account (as defined in section 19(b)(1)(C) of the Federal Reserve Act), opened at a depository institution by a foreign financial institution by means of which the foreign financial institution permits its customers to engage, either directly or through a sub-account, in banking activities usual in connection with the business of banking in the United States.

"The fourth special measure the Secretary could impose in the case of a primary money laundering concern would require domestic financial institutions, as a condition of opening or maintaining a 'correspondent' account for a foreign financial institution, to identify each customer (and representative of the customer) who is permitted to use or whose transactions flow through such an account, and to obtain for each customer (and representative) information that is substantially comparable to the information that it would obtain with respect to its own customers. With respect to a bank, the term 'correspondent account' means an account established to receive deposits from and make payments on behalf of a foreign financial institution.

"The fifth measure the Secretary could impose in the case of a primary money laundering concern would prohibit or impose conditions (beyond those already provided for in the third and fourth measures) on domestic financial institutions' correspondent or payable-through accounts with foreign banking institutions. In addition to the required consultation with the Chairman of the Board of Governors of the Federal Reserve, prior to imposing this measure the Secretary is also directed to consult with the Secretary of State and the Attorney General.

"The five special measures authorized by this section may be imposed in any sequence or combination as the Secretary determines. The first four special measures may be imposed

Due Diligence. Section 312 demands that all U.S. financial institutions have policies, procedures, and controls in place to identify instances where their correspondent and private banking accounts with foreign individuals and entities might be used for money laundering purposes, 31 U.S.C. 5318(i). They must establish enhanced due diligence standards for correspondent accounts held for offshore banking institutions (whose licenses prohibit them from conducting financial activities in the jurisdiction in which they are licensed) or institutions in money laundering jurisdictions designated by the Secretary of the Treasury or by international watch dog groups such as the Financial Action Task Force. The standards must at least involve reasonable efforts to identify the ownership of foreign institutions which are not publicly held; closely monitor the accounts for money laundering activity; and *to hold any foreign bank, for whom the U.S. institution has a correspondent account,* to the same standards with respect to other correspondent accounts maintained by the foreign bank. In the case of private banking accounts of $1 million or more, U.S. financial institutions must keep records of the owners of the accounts and the source of funds deposited in the accounts. They must report suspicious transactions and, when the accounts are held for foreign officials, guard against transactions involving foreign official corruption.[63]

---

by regulation, order, or otherwise as permitted by law. However, if the Secretary proceeds by issuing an order, the order must be accompanied by a notice of proposed rulemaking relating to the imposition of the special measure, and may not remain in effect for more than 120 days, except pursuant to a regulation prescribed on or before the end of the 120-day period. The fifth special measure may be imposed only by regulation," H.R.Rep.No. 107-250, at 68-9.

[63] *See generally,* H.R.Rep.No. 107-250, at 71-2 ("Section [312] amends 31 U.S.C. 5318 to require financial institutions that establish, maintain, administer, or manage private banking or correspondent accounts for non-U.S. persons to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls to detect and report instances of money laundering through those accounts.

"The section requires financial institutions to apply enhanced due diligence procedures when opening or maintaining a correspondent account for a foreign bank operating (1) under a license to conduct banking activities which, as a condition of the license, prohibits the licensed entity from conducting banking activities with the citizens of, or with the local currency of, the country which issued the license; or (2) under a license issued by a foreign country that has been designated (a) as non-cooperative with international anti-money laundering principles by an intergovernmental group or organization of which the United States is a member, with which designation the Secretary of the Treasury concurs, or (b) by the Secretary as warranting special measures due to money laundering concerns.

"The enhanced due diligence procedures include (1) ascertaining the identity of each of the owners of the foreign bank (except for banks that are publicly traded); (2) conducting enhanced scrutiny of the correspondent account to guard against money laundering and report any suspicious activity; and (3) ascertaining whether the foreign bank provides correspondent accounts to other foreign banks and, if so, the identity of those foreign banks and related due diligence information.

"For private banking accounts requested or maintained by a non-United States person, a financial institution is required to implement procedures for (1) ascertaining the identity of the nominal and beneficial owners of, and the source of funds deposited into, the account as needed to guard against money laundering and report suspicious activity; and (2) conducting enhanced scrutiny of any such account requested or maintained by, or on behalf of, a senior foreign political figure, or his immediate family members or close associates, to prevent,

General Regulatory Matters. The Act establishes several other regulatory mechanisms directed at the activities involving U.S. financial institutions and foreign individuals or institutions. Section 313, for instance, in another restriction on correspondent accounts for foreign financial institutions, prohibits U.S. financial institutions from maintaining correspondent accounts either directly or indirectly for foreign shell banks (banks with no physical place of business[64]) which have no affiliation with any financial institution through which their banking activities are subject to regulatory supervision.[65]

The Act, in section 325, empowers the Secretary of the Treasury to promulgate regulations to prevent financial institutions from allowing their customers to conceal their financial activities by taking advantage of the institutions' concentration account practices.[66]

The Secretary of the Treasury is instructed in section 326 to issue regulations for financial institutions' minimum new customer identification standards and record-

---

detect and report transactions that may involve the proceeds of foreign corruption. A private bank account is defined as an account (or any combination of accounts) that requires a minimum aggregate deposit of funds or other assets of not less than $1 million; is established on behalf of one or more individuals who have a direct or beneficial ownership in the account; and is assigned to, or administered or managed by, an officer, employee or agent of a financial institution acting as a liaison between the institution and the direct or beneficial owner of the account.

"This section directs the Secretary of the Treasury, within 6 months of enactment of this bill and in consultation with appropriate Federal functional regulators, to further define and clarify, by regulation, the requirements imposed by this section").

[64] Or more exactly, a bank which has no physical presence in any country; a "physical presence" for a foreign bank is defined as "a place of business that – (i) is maintained by a foreign bank; (ii) is located at a fixed address (other than solely an electronic address) in a country in which the foreign bank is authorized to conduct banking activities, at which location the foreign bank – (I) employs 1 or more individuals on a full-time basis; and (II) maintains operating records relating to its banking activities; and (iii) is subject to inspection by the banking authority which licensed the foreign bank to conduct banking activities," 31 U.S.C. 5318(j)(4).

[65] 31 U.S.C. 5318(j); H.R.Rep.No. 107-250, at 72 (2001).

[66] The Act does not define "concentration accounts," although the House Financial Services Committee report provides some incite into the section's intent, H.R.Rep.No. 107-250, at 72-3 (2001)("This section gives the Secretary of the Treasury discretionary authority to prescribe regulations governing the maintenance of concentration accounts by financial institutions, to ensure that these accounts are not used to prevent association of the identity of an individual customer with the movement of funds of which the customer is the direct or beneficial owner. If promulgated, the regulations are required to prohibit financial institutions from allowing clients to direct transactions into, out of, or through the concentration accounts of the institution; prohibit financial institutions and their employees from informing customers of the existence of, or means of identifying, the concentration accounts of the institution; and to establish written procedures governing the documentation of all transactions involving a concentration account.")

keeping and to recommend a means to effectively verify the identification of foreign customers.[67]

---

[67] 31 U.S.C. 5318(*l*); H.R.Rep.No. 107-250, at 62-3 (2001)("Section [326](a) amends 31 U.S.C. 5318 by adding a new subsection governing the identification of account holders. Paragraph (1) directs Treasury to prescribe regulations setting forth minimum standards for customer identification by financial institutions in connection with the opening of an account. By referencing 'customers' in this section, the Committee intends that the regulations prescribed by Treasury take an approach similar to that of regulations promulgated under title V of the Gramm-Leach-Bliley Act of 1999, where the functional regulators defined 'customers' and 'customer relationship' for purposes of the financial privacy rules. Under this approach, for example, where a mutual fund sells its shares to the public through a broker-dealer and maintains a 'street name' or omnibus account in the broker-dealer's name, the individual purchasers of the fund shares are customers of the broker-dealer, rather than the mutual fund. The mutual fund would not be required to 'look through' the broker-dealer to identify and verify the identities of those customers. Similarly, where a mutual fund sells its shares to a qualified retirement plan, the plan, and not its participants, would be the fund's customers. Thus, the fund would not be required to 'look through' the plan to identify its participants.

"Paragraph (2) requires that the regulations must, at a minimum, require financial institutions to implement procedures to verify (to the extent reasonable and practicable) the identity of any person seeking to open an account, maintain records of the information used to do so, and consult applicable lists of known or suspected terrorists or terrorist organizations. The lists of known or suspected terrorists that the Committee intends financial institutions to consult are those already supplied to financial institutions by the Office of Foreign Asset Control (OFAC), and occasionally by law enforcement and regulatory authorities, as in the days immediately following the September 11, 2001, attacks on the World Trade Center and the Pentagon. It is the Committee's intent that the verification procedures prescribed by Treasury make use of information currently obtained by most financial institutions in the account opening process. It is not the Committee's intent for the regulations to require verification procedures that are prohibitively expensive or impractical.

"Paragraph (3) requires that Treasury consider the various types of accounts maintained by various financial institutions, the various methods of opening accounts, and the various types of identifying information available in promulgating its regulations. This would require Treasury to consider, for example, the feasibility of obtaining particular types of information for accounts opened through the mail, electronically, or in other situations where the accountholder is not physically present at the financial institution. Millions of Americans open accounts at mutual funds, broker-dealers, and other financial institutions in this manner; it is not the Committee's intent that the regulations adopted pursuant to this legislation impose burdens that would make this prohibitively expensive or impractical. This provision allows Treasury to adopt regulations that are appropriately tailored to these types of accounts.

"Current regulatory guidance instructs depository institutions to make reasonable efforts to determine the true identity of all customers requesting an institution's services. (See, e.g., FDIC Division of Supervision Manual of Exam Policies, section 9.4 VI.) The Committee intends that the regulations prescribed under this section adopt a similar approach, and impose requirements appropriate to the size, location, and type of business of an institution.

"Paragraph (4) requires that Treasury consult with the appropriate functional regulator in developing the regulations. This will help ensure that the regulations are appropriately tailored to the business practices of various types of financial institutions, and the risks that such practices may pose.

"Paragraph (5) gives each functional regulator the authority to exempt, by regulation or order, any financial institution or type of account from the regulations prescribed under paragraph (1).

Federal regulatory authorities must approve the merger of various financial institutions under the Bank Holding Company Act, 12 U.S.C. 1842, and the Federal Deposit Insurance Act, 12 U.S.C. 1828. Section 327 requires consideration of an institution's anti-money laundering record when such mergers are proposed, 12 U.S.C. 1842(c)(6), 1828(c)(11).

Section 314 directs the Secretary of the Treasury to promulgate regulations in order to encourage financial institutions and law enforcement agencies to share information concerning suspected money laundering and terrorist activities, 31 U.S.C. 5311 note.

Section 319(b) requires U.S. financial institutions to respond to bank regulatory authorities' requests for anti-money laundering records (within 120 hours) and to Justice or Treasury Department subpoenas or summons for records concerning foreign deposits (within 7 days), 31 U.S.C. 5318(k). Section 319 also calls for civil penalties of up to $10,000 a day for financial institutions who have failed to terminate correspondent accounts with foreign institutions that have ignored Treasury or Justice Department subpoenas or summons, 31 U.S.C. 5318(k)(3).

Section 352 directs the Secretary of the Treasury to promulgate regulations, in consultation with other appropriate regulatory authorities, requiring financial institutions to maintain anti-money laundering programs which must include at least a compliance officer; an employee training program; the development of internal policies, procedures and controls; and an independent audit feature.[68]

Section 359 subjects money transmitters to the regulations and requirements of the Currency and Foreign Transactions Reporting Act (31 U.S.C. 5311 et seq.) and directs the Secretary of the Treasury to report on the need for additional legislation relating to domestic and international underground banking systems.

Federal law obligates the Administration to develop a national strategy for combating money laundering and related financial crimes, 31 U.S.C. 5341. Section 354 insists that the strategy contain data relating to the funding of international terrorism and efforts to prevent, detect, and prosecute such funding, 31 U.S.C. 5341(b)(12).

Section 364 authorizes the Board of Governors of the Federal Reserve to hire guards to protect members of the Board, as well as the Board's property and personnel and that of any Federal Reserve bank. The guards may carry firearms and make arrests, 12 U.S.C. 248(q).

Reports to Congress. Section 366 instructs the Secretary of the Treasury to report on methods of improving the compliance of financial institutions with the currency transaction reporting requirements and on the possibility of expanding

---

"Paragraph (6) requires that Treasury's regulations prescribed under paragraph (1) become effective within one year after enactment of this bill").

[68] 31 U.S.C. 5318(h); H.R.Rep.No. 107-250, at 72 (2001).

exemptions to the requirements with an eye to improving the quality of data available for law enforcement purposes and reducing the number of unnecessary filings.[69]

Section 324 instructs the Secretary of the Treasury to report on the execution of authority granted under the International Counter Money Laundering and Related Measures subtitle (III-A) of the Act and to recommend any appropriate related legislation, 31 U.S.C. 5311 note.

International Cooperation. Reflecting concern about the ability of law enforcement officials to trace money transfers to this country from overseas, section 328 instructs the Secretary of the Treasury, Secretary of State and Attorney General to make every effort to encourage other governments to require identification of the originator of international wire transfers.[70]

Section 330 expresses the sense of the Congress that the Administration should seek to negotiate international agreements to enable U.S. law enforcement officials to track the financial activities of foreign terrorist organizations, money launderers and other criminals.

Section 360 authorizes the Secretary of the Treasury to direct the U.S. Executive Directors of the various international financial institutions (*i.e.*, the International Monetary Fund, the International Bank for Reconstruction and Development, the European Bank for Reconstruction and Development, the International Development Association, the International Finance Corporation, the Multilateral Investment Guarantee Agency, the African Development Bank, the African Development Fund, the Asian Development Bank, the Bank for Economic Development and Cooperation in the Middle East and North Africa, and the InterAmerican Investment Corporation): (1) to support the loan and other benefit efforts on behalf of countries that the President determines have supported our anti-terrorism efforts, and (2) to vote to ensure that funds from those institutions are not used to support terrorism.

---

[69] 31 U.S.C. 5313 note; H.R.Rep.No. 107-205, at 65 (2001).

[70] H.R.Rep.No. 107-250, at 67 (2001)("This section directs the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to (1) take all reasonable steps to encourage foreign governments to require the inclusion of the name of the originator in wire transfer instructions sent to the U.S. and other countries; and (2) report annually to Congress on Treasury's progress in achieving this objective, and on impediments to instituting a regime in which all appropriate identification about wire transfer recipients is included with wire transfers from their point of origination until disbursement.

"The Committee is concerned that inadequate information on the originator of wire transfers from a number of foreign jurisdictions makes it difficult for both law enforcement and financial institutions to properly understand the source of funds entering the United States in wire transfers. Such a lack of clarity could aid money launderers or terrorists in moving their funds into the United States financial system. Additionally, while arguments have been made that there are technical impediments to requiring that complete addressee information appear on all wire transfers terminating in or passing through the United States, the Committee believes that having such information is technically feasible and would aid both financial institutions in performing due diligence and law enforcement in tracking or seizing money that is the derivative of or would be used in the commission of a crime").

Crimes. Federal criminal money laundering statutes punish both concealing the fruits of old offenses and financing new ones. They proscribe financial transactions which:

- involve more than $10,000 derived from one of a list of specified underlying crimes, 18 U.S.C. 1957, or
- are intended to promote any of the designated predicate offenses, or
- are intended to evade taxes, or
- are designed to conceal the proceeds generated by any of the predicate offenses, or
- are crafted to avoid transaction reporting requirements, 18 U.S.C. 1956.

They also condemn transporting funds into, out of, or through the United States with the intent to further a predicate offense, conceal its proceeds, or evade reporting requirements, 18 U.S.C. 1956. Offenders face imprisonment for up to twenty years, fines of up to $500,000, civil penalties, 18 U.S.C. 1956, 1957, and confiscation of the illicit funds involved in a violation or in any of the predicate offenses, 18 U.S.C. 981, 982.

The Act contains a number of new money laundering crimes, as well as amendments and increased penalties for existing crimes. Section 315, for example, adds several crimes to the federal money laundering predicate offense list of 18 U.S.C. 1956. The newly added predicate offenses include crimes in violation of the laws of the other nations when the proceeds are involved in financial transactions in this country: crimes of violence, public corruption, smuggling, and offenses condemned in treaties to which we are a party, 18 U.S.C. 1956(c)(7)(B). Additional federal crimes also join the predicate list:

- 18 U.S.C. 541 (goods falsely classified)
- 18 U.S.C. 922(1) (unlawful importation of firearms)
- 18 U.S.C. 924(n) (firearms trafficking)
- 18 U.S.C. 1030 (computer fraud and abuse)
- felony violations of the Foreign Agents Registration Act, 22 U.S.C. 618.

As the report accompanying H.R. 3004 explains:

> This amendment enlarges the list of foreign crimes that can lead to money laundering prosecutions in this country when the proceeds of additional foreign crimes are laundered in the United States. The additional crimes include all crimes of violence, public corruption, and offenses covered by existing bilateral extradition treaties. The Committee intends this provision to send a strong signal that the United States will not tolerate the use of its financial institutions for the purpose of laundering the proceeds of such activities. H.R.Rep.No. 107-250, at 55 (2000).

In this same vein, section 376 adds the crime of providing material support to a terrorist organization (18 U.S.C. 2339B) to the predicate offense list and section 318

expands 18 U.S.C. 1956 to cover financial transactions conducted in foreign financial institutions.[71]

Section 329 makes it a federal crime to corruptly administer the money laundering regulatory scheme. Offenders are punishable by imprisonment for not more than 15 years and a fine of not more than three times the amount of the bribe.

Section 5326 of title 31 authorizes the Secretary of the Treasury to impose temporary, enhanced reporting requirements upon financial institutions in areas victimized by substantial money laundering activity (geographic targeting regulations and orders). Section 353 makes it clear that the civil sanctions, criminal penalties, and prohibitions on smurfing (structuring transactions to evade reporting requirements) apply to violations of the regulations and orders issued under 31 U.S.C. 5326.[72] It also extends the permissible length of the temporary geographical orders from 60 to 180 days.

Violations of the special measures and special due diligence requirements of sections 311 and 312 are subject to both civil and criminal penalties by virtue of section 363's amendments to 31 U.S.C. 5321(a) and 5322. The amendments authorize civil penalties and criminal fines of twice the amount of the transaction but not more than $1 million. Criminal offenders would be subject to a fine in the same amount.

---

[71] "[S]ection 1956 of title 18, United States Code, makes it an offense to conduct a transaction involving a financial institution if the transaction involves criminally derived property. Similarly, 18 U.S.C. 1957 creates an offense relating to the deposit, withdrawal, transfer or exchange of criminally derived funds 'by, to or through a financial institution.' For the purposes of both statutes, the term 'financial institution' is defined in 31 U.S.C. 5312. See 18 U.S.C. 1956(c)(6); 18 U.S.C. 1957(f).

"The definition of 'financial institution' in 5312 does not explicitly include foreign banks. Such banks may well be covered because they fall within the meaning of 'commercial bank' or other terms in the statute, but as presently drafted, there is some confusion over whether the government can rely on section 5312 to prosecute an offense under either 1956 or 1957 involving a transaction through a foreign bank, even if the offense occurs in part in the United States. For example, if a person in the United States sends criminal proceeds abroad--say to a Mexican bank--and launders them through a series of financial transactions, the government conceivably could not rely on the definition of a 'financial institution' in 1956(c)(6) to establish that the transaction was a 'financial transaction' within the meaning of 1956(c)(4)(B) (defining a 'financial transaction' as a transaction involving the use of a 'financial institution'), or that it was a 'monetary transaction' within the meaning of 1957(f) (defining 'monetary transaction' as, inter alia, a transaction that would be a 'financial transaction' under 1956(c)(4)(B)).

"Similarly, the money laundering laws in effect in most countries simply make it an offense to launder the proceeds of any crime, foreign or domestic. In the United States, however, the money laundering statute is violated only when a person launders the proceeds of one of the crimes set forth on a list of 'specified unlawful activities.' 18 U.S.C. 1956(c)(7). Currently only a handful of foreign crimes appear on that list. See 1956(c)(7)(B)," H.R.Rep.No. 107-250, at 38 (2000).

[72] *Cf.,* H.R.Rep.No. 107-250, at 57.

Earlier federal law prohibited the operation of illegal money transmitting businesses, 18 U.S.C. 1960. Section 373 amends the proscription to make it clear that the prohibition must be breached "knowingly" and to cover businesses which are otherwise lawful but which transmit funds they know are derived from or intended for illegal activities. It also amends 18 U.S.C. 981(a)(1)(A) to permit civil forfeiture of property involved in a transaction in violation of 18 U.S.C. 1960.[73]

Sections 374 and 375 of the Act seek to curtail economic terrorism by increasing and making more uniform the penalties for counterfeiting U.S. or foreign currency and by making it clear that the prohibitions against possession of counterfeiting paraphernalia extend to their electronic equivalents.[74] They increase the maximum terms of imprisonment for violation of:

- 18 U.S.C. 471 (obligations or securities of the U.S.) from 15 to 20 years;
- 18 U.S.C. 472 (uttering counterfeit obligations and securities) from 15 to 20 years;
- 18 U.S.C. 473 (dealing in counterfeit obligations and securities) from 10 to 20 years;

---

[73] "The operation of an unlicensed money transmitting business is a violation of Federal law under 18 U.S.C. 1960. First, section 104 clarifies the scienter requirement in 1960 to avoid the problems that occurred when the Supreme Court interpreted the currency transaction reporting statutes to require proof that the defendant knew that structuring a cash transaction to avoid the reporting requirements had been made a criminal offense. See Ratzlaf v. United States, 114 S. Ct. 655 (1994). The proposal makes clear that an offense under 1960 is a general intent crime for which a defendant is liable if he knowingly operates an unlicensed money transmitting business. For purposes of a criminal prosecution, the Government would not have to show that the defendant knew that a State license was required or that the Federal registration requirements promulgated pursuant to 31 U.S.C. 5330 applied to the business.

"Second, section 104 expands the definition of an unlicensed money transmitting business to include a business engaged in the transportation or transmission of funds that the defendant knows are derived from a criminal offense, or are intended to be used for an unlawful purpose. Thus, a person who agrees to transmit or to transport drug proceeds for a drug dealer, or funds from any source for a terrorist, knowing such funds are to be used to commit a terrorist act, would be engaged in the operation of an unlicensed money transmitting business. It would not be necessary for the Government to show that the business was a storefront or other formal business open to walk-in trade. To the contrary, it would be sufficient to show that the defendant offered his services as a money transmitter to another.

"Finally, when Congress enacted 1960 in 1992, it provided for criminal but not civil forfeiture. The proposal corrects this oversight, and allows the government to obtain forfeiture of property involved in the operation of an illegal money transmitting business even if the perpetrator is a fugitive," H.R.Rep.No. 107-250, at 54 (2001).

[74] "This section makes it a criminal offense to possess an electronic image of an obligation or security document of the United States with intent to defraud. The provision harmonizes counterfeiting language to clarify that possessing either analog or digital copies with intent to defraud constitutes an offense. This section mimics existing language that makes it a felony to possess the plates from which currency can be printed, and takes into account the fact that most counterfeit currency seized today is generated by computers or computer-based equipment. The section also increases maximum sentences for a series of counterfeiting offenses," H.R.Rep.No. 107-250, at 75-6 (2001).

- 18 U.S.C. 476 (taking impressions of tools used for obligations and securities) from 10 to 25 years;
- 18 U.S.C. 477 (possessing or selling impressions of tools used for obligations or securities) from 10 to 25 years;
- 18 U.S.C. 484 (connecting parts of different notes) from 5 to 10 years;
- 18 U.S.C. 493 (bonds and obligations of certain lending agencies) from 5 to 10 years;
- 18 U.S.C. 478 (foreign obligations or securities) from 5 to 20 years;
- 18 U.S.C. 479 (uttering counterfeit foreign obligations or securities) from 3 to 20 years;
- 18 U.S.C. 480 (possessing counterfeit foreign obligations or securities) from 1 to 20 years;
- 18 U.S.C. 481 (plates, stones, or analog, digital, or electronic images for counterfeiting foreign obligations or securities) from 5 to 25 years;
- 18 U.S.C. 482 (foreign bank notes) from 2 to 20 years; and
- 18 U.S.C. 483 (uttering counterfeit foreign bank notes) from 1 to 20 years.

Aliens believed to have engaged in money laundering may not enter the United States, section 1006 (8 U.S.C. 1182(a)(2)(I)). The same section directs the Secretary of State to maintain a watchlist to ensure that they are not admitted, 8 U.S.C. 1182 note.

Bulk Cash. Customs officials ask travelers leaving the United States whether they are taking $10,000 or more in cash with them. Section 1001 of title 18 of the United States Code makes a false response punishable by imprisonment for not more than 5 years. Section 5322 of title 31 makes failure to report taking $10,000 or more to or from the United States punishable by the same penalties. The Act's bulk cash smuggling offense, section 371, augments these proscriptions with a somewhat unique feature, 31 U.S.C. 5332 – a criminal forfeiture of the smuggled cash in lieu of a criminal fine. The basic offense outlaws smuggling cash into or out of the United States. The concealment element of the offense seems to cover everything but in-sight possession as long as an amount $10,000 or more is carried in manner to evade reporting.[75]

The section appears to be the product of reactions to the Supreme Court's decision in *United States v. Bajakian*, 524 U.S. 321 (1998). There officials had confiscation $350,000 because Bajakian attempted to leave the country without declaring it, a violation of 31 U.S.C. 5322. In the view of the Court, the confiscation was grossly disproportionate to the gravity of the offense and consequently contrary to the Constitution's excessive fines clause, 524 U.S. at 337. The Committee Report accompanying H.R. 3004 explains the Justice Department's assurance that casting surreptitious removal of cash from the United States as a smuggling rather than a false reporting offense will avoid the adverse consequences of the Supreme Court's

[75] "For purposes of this section, the concealment of currency on the person of any individual includes concealment in any article of clothing worn by the individual or in any luggage, backpack, or other container worn or carried by such individual," 31 U.S.C. 5332(a)(2).

examination of forfeiture in false reporting cases under the Constitution's Excessive Fines Clause.[76]

Section 5317 of title 31 once called for civil forfeiture of property traceable to a violation of 31 U.S.C. 5316 (reports on exporting or importing money instruments worth $10,000 or more). Section 372 of the Act recasts section 5317 to provide for civil and criminal forfeitures for violations of 31 U.S.C. 5316, of 31 U.S.C. 5313 (reports on domestic coins and currency transactions involving $10,000 or more) and of 31 U.S.C. 5324 (structuring transactions to evade reporting requirements (smurfing)).

Extraterritorial Jurisdiction. The Act makes 18 U.S.C. 1029, the federal statute condemning various crimes involving credit cards, PIN numbers and other access devices, applicable overseas if the card or device is issued by or controlled by an American bank or other entity *and* some article is held in or transported to or through the United States during the course of the offense, section 377. The change was part of the original Justice Department proposals. Justice explained that, "[financial crime[] admits of no border, utilizing the integrated global financial network for ill purposes. This provision would apply the financial crimes prohibitions to conduct committed abroad, so long as the tools or proceeds of the crimes pass through or are in the United States," *DoJ* at §408. The section, however, appears to limit the otherwise applicable extraterritorial jurisdiction implicit in section 1029, since federal courts would likely recognize extraterritorial jurisdiction over a violation

---

[76] "As recent Congressional hearings have demonstrated, currency smuggling is an extremely serious law enforcement problem. Hundreds of millions of dollars in U.S. currency – representing the proceeds of drug trafficking and other criminal offenses – is annually transported out of the United States to foreign countries in shipments of bulk cash. Smugglers use all available means to transport the currency out of the country, from false bottoms in personal luggage, to secret compartments in automobiles, to concealment in durable goods exported for sale abroad. . . .

"Presently, the only law enforcement weapon against such smuggling is section 5316 of title 31, United States Code, which makes it an offense to transport more than $10,000 in currency or monetary instruments into, or out of, the United State without filing a report with the United States Customs Service. The effectiveness of section 5316 as a law enforcement tool has been diminished, however, by a recent Supreme Court decision. In *United States v. Bajakajian*, 118 S.Ct. 2028 (1998), the Supreme Court held that section 5316 constitutes a mere reporting violation, which is not a serious offense for purposes of the Excessive Fines Clause of the Eighth Amendment. Accordingly, confiscation of the full amount of the smuggled currency is unconstitutional, even if the smuggler took elaborate steps to conceal the currency and otherwise obstruct justice.

"Confiscation of the smuggled currency is, of course, the most effective weapon that can be employed against currency smugglers. Accordingly, in response to the *Bajakajian* decision, the Department of Justice proposed making the act of bulk cash smuggling itself a criminal offense, and to authorize the imposition of the full range of civil and criminal sanctions when the offense is discovered. Because the act of concealing currency for the purpose of smuggling it out of the United States is inherently more serious than simply failing to file aC ustoms report, strong and meaningful sanctions, such as confiscation of the smuggled currency, are likely to withstand Eighth Amendment challenges to the new statute," H.R.Rep.No. 107-250 at 36-7 (2001).

under *either* circumstance (issued by a U.S. entity or physical presence in the U.S.) as well as a number of others.[77]

Venue. Section 1004 relies on *dicta* in *United States v. Cabrales*, 524 U.S. 1, 8 (1998), in order to permit a money laundering prosecution to be brought in the place where the crime which generated the funds occurred, "if the defendant participated in the transfer of the proceeds," 18 U.S.C. 1956(i).

Ordinarily, the Constitution requires that a crime be prosecuted in the state and district in which it occurs, in the case of money laundering,[78] in the state and district in which the monetary transaction takes place. The Supreme Court in *Cabrales* held that a charge of money laundering in Florida, of the proceeds of a Missouri drug trafficking, could not be tried in Missouri. The Court declared in *dicta*, however, that "money laundering . . . arguably might rank as a continuing offense, triable in more than one place, if the launderer acquired the funds in one district and transported them into another," 524 U.S. at 8.[79]

Forfeiture. Forfeiture is the government confiscation of property as a consequence of crime.[80] The forfeiture amendments of the Act fall into two categories. Some make adjustments to those portions of federal forfeiture law which govern the confiscation of property derived from, or used to facilitate, various federal crimes. Others follow the pattern used for the war-time confiscation of the property of enemy aliens under the Trading With the Enemy Act, 50 U.S.C.App. 1 *et seq.* (TWEA), forfeitures which turn on the ownership of the property rather than upon its proximity to any particular crime.

Constitutional Considerations. The Act adds TWEA-like amendments to the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. 1701 *et seq.*, which already allowed the President to freeze the assets of foreign terrorists under certain conditions. Under IEEPA, as amended by section 106 of the Act, the President or his delegate may confiscate and dispose of any property, within the

---

[77] *United States v. Bowman*, 260 U.S. 94, 97-8 (1922); *Ford v. United States*, 273 U.S. 593, 623 (1927). For a general discussion of the extraterritorial application of federal criminal law, *see,* Doyle, *Extraterritorial Application of American Criminal Law*, CRS REP.NO. 94-166A (Mar. 13, 1999).

[78] "The trial of all crimes . . . shall be held in the state where the said crimes shall have been committed; but when not committed within any state, the trial shall be at such place or places as the Congress may by law have directed," *U.S.Const.* Art.III, §2, cl.3.

"[I]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed; which district shall have been previously ascertained by law," *U.S.Const.* Amend. VI.

[79] *See also, United States v. Rodriguez-Moreno*, 526 U.S. 275, 280-81 n.4 (1999) (holding that acquiring and using a firearm in Maryland in connection with a kidnaping in New Jersey might constitutionally be prosecuted in New Jersey under a statute which outlawed possession of a firearm "during and in relation to" a crime of violence.

[80] For general background information, *see*, Doyle, *Crime and Forfeiture*, CRS REP.NO. 97-139A (Oct. 11, 2000).

jurisdiction of the United States, belonging to any foreign individual, foreign entity, or foreign country whom they determine to have planned, authorized, aided or engaged in an attack on the United States by a foreign country or foreign nationals. The section also permits the government to present secretly (ex parte and in camera) any classified information upon which the forfeiture was based should the decision be subject to judicial review. The Justice Department requested the section as a revival of the President's powers in times of unconventional wars.[81] By virtue of section 316, property owners may initiate a challenge to a confiscation by filing a claim under the rules applicable in maritime confiscations. The section permits two defenses to forfeiture – that the property is not subject to confiscation under section 106 or that the claimant is entitled to the innocent owner defense of 18 U.S.C. 983(d).[82] The characterization of the defenses as "affirmative defense" indicates that the claimant bears the burden of proof. The innocent owner defenses of 18 U.S.C. 983(d) are probably not available in cases under section 106, since that section is explicitly

---

[81] "This section is designed to accomplish two principal objectives. First, the section restores to the President, in limited circumstances involving armed hostilities or attacks against the United States, the power to confiscate and vest in the United States property of enemies during times of national emergency, which was contained in the Trading with the Enemy Act, 50 App. U.S.C. §5(b)(TWEA) until 1977. Until the International Economic Emergency Act (IEEPA) was passed in 1977, section 5(b) permitted the President to vest enemy property in the United States during time of war *or* national emergency. When IEEPA was passed, it did not expressly include a provision permitting the vesting of property in the United States, and section 5(b) of TWEA was amended to apply only 'during the time of war.' 50 App.U.S.C. §5(b).

"This new provision tracks the vesting language currently in section 5(b) of TWEA and permits the President, only in the limited circumstances when the United States is engaged in military hostilities or has been subject to an attack, to confiscate property of any foreign country, person, or organization involved in hostilities or attacks on the United States. Like the original provision in TWEA, it is an exercise of Congress's war power under Article I, section 8, clause 11 of the Constitution and is designed to apply to unconventional warfare where Congress has not formally declared war against a foreign nation.

"The second principal purpose of this amendment to IEEPA is to ensure that reviewing courts may base their rulings on an examination of the complete administrative record in sensitive national security or terrorism cases without requiring the United States to compromise classified information. New section (c) would authorize a reviewing court, in the process of verifying that determinations made by the executive branch were based upon substantial evidence and were not arbitrary or capricious, to consider classified evidence ex parte and in camera. This would ensure that reviewing courts have the best and most complete information upon which to base their decisions without forcing the United States to choose between compromising highly sensitive intelligence information or declining to take action against individuals or entities that may present a serious threat to the United States or its nationals. A similar accommodation mechanism was enacted by Congress in the Anti-Terrorism and Effective Death Penalty Act of 1996, 8 U.S.C. §1189(b)(2)," *DoJ* at §159.

[82] "An owner of property that is confiscated under any provision of law relating to the confiscation of assets of suspected international terrorists, may contest that confiscation by filing a claim in the manner set forth in the Federal Rules of Civil Procedure (Supplemental Rules for Certain Admiralty and Maritime Claims), and asserting as an affirmative defense that – (1) the property is not subject to confiscation under such provision of law; or (2) the innocent owner provisions of section 983(d) of title 18, United States Code, apply to the case," Sec. 316(a).

excepted from the coverage of 18 U.S.C. 983.[83] The challenge proceedings permit the court to admit evidence, such as hearsay evidence, that would not otherwise be admissible under the Federal Rules of Evidence if the evidence is reliable and if national security might be imperiled should dictates of the Federal Rules be followed, §316(b). The section recognizes the rights of claimants to proceed alternatively under the Constitution or the Administrative Procedure Act.[84]

The Justice Department also recommended enactment of an overlapping provision which ultimately passed as section 806 of the Act without any real discussion of the relationship of the two sections.[85] Section 806 authorizes confiscation of all property, regardless of where it is found, of any individual, entity, or organization engaged in domestic or international terrorism (as defined in 18 U.S.C. 2331),[86] against the United States, Americans or their property, 18 U.S.C.

---

[83] 18 U.S.C. 983(i)(2)(D).

[84] "The exclusion of certain provisions of Federal law from the definition of the term 'civil forfeiture statute' in section 983(i) of title 18, United States Code, shall not be construed to deny an owner of property the right to contest the confiscation of assets of suspected international terrorists under – (A) subsection (a) of this section; (B) the Constitution; or (C) subschapter II of chapter 5 of title 5, United States Code (commonly known as the 'Administrative Procedure Act')," Sec. 316(c)(1).

[85] "Current law does not contain any authority tailored specifically to the confiscation of terrorist assets. Instead, currently, forfeiture is authorized only in narrow circumstances for the proceeds of murder, arson, and some terrorism offenses, or for laundering the proceeds of such offenses. However, most terrorism offenses do not yield 'proceeds,' and available current forfeiture laws require detailed tracing that is quite difficult for accounts coming through the banks of countries used by many terrorists.

"This section increases the government's ability to strike at terrorist organizations' economic base by permitting the forfeiture of its property regardless of the source of the property, and regardless of whether the property has actually been used to commit a terrorism offense. This is similar in concept to the forfeiture now available under RICO. In parity with the drug forfeiture laws, the section also authorizes the forfeiture of property used or intended to be used to facilitate a terrorist act, regardless of its source. There is no need for a separate criminal forfeiture provision because criminal forfeiture is incorporated under current law by reference. The provision is retroactive to permit it to be applied to the events of September 11, 2001," *DoJ*, at §403. The House Report on H.R. 2975 which contained versions of both sections is no more explicit on the relation of the two sections.

[86] "(1) the term 'international terrorism' means activities that – (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum . . . (5) the term 'domestic terrorism' means activities that – (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct

981(a)(1)(G). Section 806 as discussed below also calls for the more common confiscation of property derived from and or facilitating acts of domestic or international terrorism against the United States or its citizens. Confiscations under 806 may be challenged under the procedures of 18 U.S.C. 983, since they are not exempted there. To the extent that forfeiture under section 806 is based on international rather than domestic terrorism, claimants may also use the procedures of section 316.

Confiscation based solely on the fact that the property is owned by a criminal offender, rather than that it is derived from or facilitates some crime is fairly uncommon. It is the mark of common law forfeiture of estate. At common law, a felon forfeited all of his property. Most contemporary forfeiture statutes employ statutory forfeiture, a more familiar presence in American law,[87] which consists of the confiscation of things whose possession is criminal, of the fruits of crime, and of the means of crime – untaxed whiskey, the drug dealer's profits, and the rum runner's ship.

Three characteristics set forfeiture of estate apart. The property is lost solely by reason of its ownership by a felon. All of a felon's property is confiscated, not merely that which is related to the crime for which he is convicted. Finally, it occasions attainder which negates the felon's right to hold property or for title to property to pass through him to his heirs. It was with this in mind, that the Framers declared that "no attainder of treason shall work corruption of blood or forfeiture exception during the life of the person attainted."[88] And for this reason, President Lincoln insisted that the confiscated real estate of Confederate supporters should revert their heirs at death.[89]

---

of a government by mass destruction, assassination or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States," 18 U.S.C. 2331(1),(5)(as amended by section 802 of the Act).

[87] *Austin v. United States*, 509 U.S. 602, 611-12 (1993)("Three kinds of forfeiture were established in England at the time the Eighth Amendment was ratified in the United States: deodand, forfeiture, and statutory forfeiture . . . . Of England's three kinds of forfeiture, only the third took hold in the United States").

[88] *U.S.Const.* Art.III, §3, cl.2.

[89] 12 Stat. 589, 627 (1862). Some would suggest a fourth distinction: that it follows a felony conviction. This is hardly a distinction, since over time legislation creating statutory forfeitures has employed criminal *in personam* proceedings following criminal conviction as a means of accomplishing confiscation.

Neither section 106 nor 806 require conviction of the terrorist property owner.[90] Both call for forfeiture of all of the terrorist's property, without requiring any nexus to the terrorist's offenses other than terrorist ownership. Neither makes any explicit provision for the terrorist's heirs. Section 106 applies only to foreign persons, organizations, or countries, but section 806 recognizes no such distinction.

Of course, the Supreme Court long ago confirmed the constitutional validity of a seemingly similar pattern in TWEA under the President's war powers.[91] The Court was careful to point out, however, that the TWEA procedure was not really forfeiture or confiscation for the benefit of the United States, but by express statutory provision a liquidation measure to protect the creditors of enemy property owners.[92] Neither section 106 nor 806 are part of TWEA and neither explicitly treats the proceeds of confiscation as a fund for the benefit of creditors. Moreover, broad as the President's war powers may be, they would hardly seem to provide a justification for section 806, which embraces domestic terrorism and is neither limited to foreign offenders nor predicated upon war-like hostilities.

Criminal forfeitures, civil forfeitures with punitive as well as remedial purposes, and civil forfeitures whose effect is so punitive as to negate any presumption of remedial purpose, all raise other constitutional points of interest. The Eighth Amendment's excessive fines clause prohibits criminal forfeitures, and civil forfeitures with at least some punitive purposes, that are grossly disproportionate to the gravity of the crimes which trigger them.[93] The Fifth Amendment's double jeopardy clause applies to criminal forfeitures and civil forfeitures which are so punitive as to negate

---

[90] Although by operation of law property subject to civil forfeiture of section 806 may be confiscated upon conviction of the property owner for any crime of domestic or international terrorism, 28 U.S.C. 2461(c)("If a forfeiture of property is authorized in connection with a violation of an Act of Congress, and any person is charged in an indictment or information with such violation but no specific statutory provision is made for criminal forfeiture upon conviction, the Government may include the forfeiture in the indictment or information in accordance with the Federal Rules of Criminal Procedure, and upon conviction, the court shall order the forfeiture of the property in accordance with the procedures set forth in section 413 of the Controlled Substances Act").

[91] *Silesian American Corp. V. Clark*, 332 U.S. 469 (1947); *cf., Societe Internationale v. Rogers*, 357 U.S. 197, 211 (1958)("this summary power to seize property which is believed to be enemy-owned is rescued from constitutional invalidity under the Due Process and Just Compensation Clauses of the Fifth Amendment only by those provisions of the Act which afford a non-enemy claimant a later judicial hearing as to the propriety of the seizure").

[92] *Zittman v. McGrath*, 341 U.S. 471, 473-74 (1951)(citing 50 U.S.C.App. 34) ("While the statute under which the funds are to be 'held, administered and accounted for' authorizes the vesting of such foreign-owned property in the custodian and its administration 'in the interest of and for the benefit of the United States,' it is not a confiscation measure, but a liquidation measure for the protection of American creditors. It provides for the filing and proving of claims and states that the funds 'shall be equitably applied for the payments of debts").

[93] *United States v. Bajakajian*, 524 U.S. 321, 337 (1998); *Austin v. United States*, 509 U.S. 602, 622 (1993).

any presumption of remedial purposes.[94] The same has been said of the applicability of the ex post facto clause.[95]

The limitations on criminal forfeitures would apply to the forfeitures under section 806 when prosecuted as criminal forfeitures by operation of 28 U.S.C. 2461(c). The offenses that activate section 106 and 806 confiscations, however, are of such gravity that successful excessive fine clause challenges are unlikely, even if the value of confiscated property were extraordinarily high.

On the other hand, there is more than a little support for the argument that section 106 and 806 constitute punitive rather than remedial measures. They are potentially severe. Section 806 calls for the total impoverishment of those to whom it applies (all assets foreign and domestic), while section 106 anticipates confiscation of all assets within the jurisdiction of the United States. They seem to undermine any claim to remedial purpose by reaching those assets that neither facilitate the commission of terrorism nor constitute its fruits. Moreover, in its analysis of the language of section 806 , the Justice Department described it as conceptually akin to the criminal forfeiture provisions of RICO.[96] If the courts find section 106 or 806 are civil in name but criminal in nature, they may well conclude that efforts to enforce the sections are bound by the limitations of the double jeopardy and ex post facto clauses.

Other Forfeiture Amendments. In order to more effectively enforce money laundering penalties and prosecute civil forfeiture actions involving foreign individuals or entities, section 317 of the Act establishes a procedure for long-arm jurisdiction over individuals and entities located overseas and for the appointment of a federal receiver to take control of contested assets during the pendency of the proceedings.[97]

---

[94] *United States v. Ursery*, 518 U.S. 267, 278 (1996).

[95] *See e.g., United States v. Certain Funds (Hong Kong and Shanghai Banking Corp.)*, 96 F.3d 20, 26-7 (2d Cir. 1996). Where the ex post facto clauses do not apply, the validity of retroactive statutes is judged by due process clause standards. There is a presumption against retroactive application in such instances absent a clear indication of contrary Congressional intent grounded in the view that due process demands certain minimal notice of the law's demands, *Landgraf v. USI Film Products*, 511 U.S. 244, 265-66 (1994).

[96] *DoJ*, at §403.

[97] 18 U.S.C. 1956(b). *Cf.*, H.R.Rep.No. 107-250, at 54-5 (2001)("The first provision in this section creates a long arm statute that gives the district court jurisdiction over a foreign person, including a foreign bank, that commits a money laundering offense in the United States or converts laundered funds that have been forfeited to the Government to his own use. Thus, if the Government files a civil enforcement action under section 1956(b), or files a civil lawsuit to recover forfeited property from a third party, the district court would have jurisdiction over the defendant if the defendant has been served with process pursuant to the applicable statutes or rules of procedure, and the constitutional requirement of minimum contacts is satisfied in one of three ways: the money laundering offense took place in the United States; in the case of converted property, the property was the property of the United States by virtue of a civil or criminal forfeiture judgment; or in the case of a financial institution, the defendant maintained a correspondent bank account at another bank in the United States. Under this provision, for example, the district courts would have had jurisdiction over the defendant in the circumstances described in United States v. Swiss

In the case of inter-bank accounts where a bank in a foreign nation has an account in a bank located in the United States, section 319(a) allows seizure of funds in an account here when the foreign bank has received money laundering or drug trafficking deposits overseas.[98] Confiscation proceedings are conducted pursuant to 18 U.S.C. 953.

Federal law has for some time permitted criminal forfeiture orders to reach substitute assets if the property of the defendant subject to confiscation has become unavailable. Section 319(d) establishes a procedure under which a convicted

---

American Bank, 191 F.3d 30 (1st Cir. 1999).

"The second provision, modeled on 18 U.S.C. 1345(b), gives the district court the power to restrain property, issue seizure warrants, or take other action necessary to ensure that a defendant in an action covered by the statute does not dissipate the assets that would be needed to satisfy a judgment.

"This section also authorizes a court, on the motion of the Government or a State or Federal regulator, to appoint a receiver to gather and protect assets needed to satisfy a judgment under sections 1956 and 957, and the forfeiture provisions in sections 981 and 982. This authority is intended to apply in three circumstances: (1) when there is a judgment in a criminal case, including an order of restitution, following a conviction for a violation of section 1956 or 1957; (2) when there is a judgment in a civil case under section 1956(b) assessing a penalty for a violation of either section 1956 or 1957; and (3) when there is a civil forfeiture judgment under section 981 or a criminal forfeiture judgment, including a personal money judgment, under section 982.

"The amendment also makes section 1956(b) applicable to violations of section 1957. It applies to conduct occurring before the effective date of the Act").

[98] 18 U.S.C. 981(k). H.R.Rep.No. 107-250, at 57-8 (2001)("Section 114 creates a new provision in the civil forfeiture statute, 18 U.S.C. 981(k), authorizing the forfeiture of funds found in an interbank account. The new provision is necessary to reconcile the law regarding the forfeiture of funds in bank accounts with the realities of the global movement of electronic funds and the use of off-shore banks to insulate criminal proceeds from forfeiture. "To prevent drug dealers and other criminals from taking advantage of certain nuances of forfeiture law to insulate their property from forfeiture even though it is deposited in a bank account in the United States, it is necessary to change the law regarding the location of the debt that a bank owes to its depositor, and the identity of the real party in interest with standing to contest the forfeiture. The amendment in this section addresses the location issue by treating a deposit made into an account in a foreign bank that has a correspondent account at a U.S. bank as if the deposit had been made into the U.S. bank directly. Second, the section treats the deposit in the correspondent account as a debt owed directly to the depositor, and not as a debt owed to the respondent bank. In other words, the correspondent account is treated as if it were the foreign bank itself, and the funds in the correspondent account were debts owed to the foreign bank's customers.

"Under this arrangement, if funds traceable to criminal activity are deposited into a foreign bank, the Government may bring a forfeiture action against funds in that bank's correspondent account, and only the initial depositor, and not the intermediary bank, would have standing to contest it.

"The section authorizes the Attorney General to suspend or terminate a forfeiture in cases where there exists a conflict of laws between the U.S. and the jurisdiction in which the foreign bank is located, where such suspension or termination would be in the interest of justice and not harm U.S. national interests").

defendant may be ordered to transfer property to this country from overseas if the property is subject to confiscation.[99]

Prior to enactment of the Act, federal law permitted confiscation of any property in the United States that could be traced to a drug offense committed overseas, if the offense was punishable as a felony under the laws of the nation where it occurred and if the offense would have been a felony if committed here.[100] Section 320 enlarges this provisions to cover not only drug offenses but any of the crimes in the money laundering predicate offense list of 18 U.S.C. 1956(c)(7)(B), and continues the reciprocal felony requirements.[101] This treatment is comparable to the early coverage of the federal statute, 28 U.S.C. 2467, which permitted enforcement of foreign confiscation orders in the case of drug offenses or the crimes on the money laundering predicate offense list. Section 323 of the Act amends the foreign forfeiture enforcement statute to (1) expand the grounds for enforcement to include any crime which would have provided the grounds for confiscation had the offense been committed in the United States; (2) to authorize restraining orders to freeze the target property while enforcement litigation is pending; and (3) to limit the absence-of-timely-notice defense.[102]

---

[99] *Cf.*, H.R.Rep.No. 107-250, at 58-9 (2001) ("Section 116 authorizes a court to order a criminal defendant to repatriate his property to the United States in criminal cases. In criminal forfeiture cases, the sentencing court is authorized to order the forfeiture of 'substitute assets' when the defendant has placed the property otherwise subject to forfeiture 'beyond the jurisdiction of the court.' Frequently, this provision is applied when a defendant has transferred drug proceeds or other criminally derived property to a foreign country. In many cases, however, the defendant has no other assets in the United States of a value commensurate with the forfeitable property overseas. In such cases, ordering the forfeiture of substitute assets is a hollow sanction.

"This section amends 21 U.S.C. 853 to make clear that a court in a criminal case may issue a repatriation order--either post-trial as part of the criminal sentence and judgment, or pre-trial pursuant to the court's authority under 21 U.S.C. 853(e) to restrain property--so that they will be available for forfeiture. Failure to comply with such an order would be punishable as a contempt of court, or it could result in a sentencing enhancement, such as a longer prison term, under the U.S. Sentencing Guidelines, or both").

[100] 18 U.S.C. 981(a)(1)(B).

[101] H.R.Rep.No. 107-250, at 56 (2001)("This section is intended to reinforce the United States' compliance with the Vienna Convention. It amends 18 U.S.C. 981(a)(1)(B) to allow the United States to institute its own action against the proceeds of foreign criminal offenses when such proceeds are found in the United States. As required by the Vienna Convention, it also authorizes the confiscation of property used to facilitate such crimes. The list of foreign crimes to which this section applies is determined by cross-reference to the foreign crimes that are money laundering predicates under 1956(c)(7)(B). This section will permit the forfeiture of property involved in conduct occurring before the effective date of the Act").

[102] H.R.Rep.No. 107-250, at 59-60 (2001)("Under current law, 28 U.S.C. 2467(d) gives Federal courts the authority to enforce civil and criminal forfeiture judgments entered by foreign courts. This section amends that provision to include a mechanism for preserving property subject to forfeiture in a foreign country.

"Specifically, a Federal court could issue a restraining order under 18 U.S.C. 983(j) or register and enforce a foreign restraining order, if the Attorney General certified that such foreign order was obtained in accordance with the principles of due process. A person seeking

A fugitive may not challenge a federal forfeiture.[103] Section 322 applies this fugitive disentitlement to corporations whose major shareholder is a fugitive or whose representative in the confiscation proceedings is a fugitive.

Section 906 instructs the Attorney General, the Secretary of the Treasury, and the Director of Central Intelligence to submit a joint report with recommendations relating to the reconfiguration of the Foreign Terrorist Asset Tracking Center, the Office of Foreign Assets Control, and possibly FinCEN in "order to establish a capability to provide for the effective and efficient analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations."

---

to contest the restraining order could do so on the ground that 28 U.S.C. 2467 was not properly applied to the particular case, but could not oppose the restraining order on any ground that could also be raised in the proceedings pending in a foreign court. This provision prevents a litigant from taking 'two bites at the apple' by raising objections to the basis for the forfeiture in the Federal court that he also raised, or is entitled to raise, in the foreign court where the forfeiture action is pending. It complements the existing provision in section 2467(e) providing that the Federal court is bound by the findings of fact of the foreign court, and may not look behind such findings in determining whether to enter an order enforcing a foreign forfeiture judgment.

"This section also amends 28 U.S.C. 2467 to make clear that it is not necessary to prove that the person asserting an interest in the property received actual notice of the forfeiture proceedings. As is the case with respect to forfeitures under U.S. law, it is sufficient if the foreign nation takes steps to provide notice, in accordance with the principles of due process. See Gonzalez v. United States, 1997 WL 278123 (S.D.N.Y. 1997) ('the [G]overnment is not required to ensure actual receipt of notice that is properly mailed'); Albajon v. Gugliotta , 72 F. Supp. 2d 1362 (S.D. Fla. 1999) (notice sent to various addresses on claimant's identifications, and mailed after claimant released from jail, is sufficient to satisfy due process, even if claimant never received notice); United States v. Schiavo , 897 F. Supp. 644, 648 49 (D. Mass. 1995) (sending notice to fugitive's last known address is sufficient; due process satisfied even if he did not receive the notice).

"Finally, 28 U.S.C. 2467 is amended to authorize the enforcement of a forfeiture judgment based on any foreign offense that would constitute an offense giving rise to a civil or criminal forfeiture of the same property if the offense had been committed in the United States. This is one of two safeguards that the statute contains against the enforcement of judgments that the United States does not consider appropriate for enforcement: if the judgment is based on an act that would not constitute a crime in the United States, such as removing assets from the reach of a repressive regime, it could not be enforced. In addition, section 2467 already provides that a foreign judgment may only be enforced by a Federal court at the request of the United States, and only after the Attorney General has certified that the judgment was obtained in accordance with the principles of due process. Thus, neither a foreign Government nor a foreign private party could enforce a foreign judgment on its own under this provision."). Note that the safeguard to which the report refers is the range of foreign offenses that will support an enforceable confiscation order, *i.e.,* drug offenses and crimes on the money laundering predicate offense list, and that the amendment narrows that safeguard by adding additional foreign offenses, *i.e.*, any foreign equivalent of a federal crime which would support a confiscation order.

[103] 28 U.S.C. 2466.

Alien Terrorists and Victims

The Act contains a number of provisions designed to prevent alien terrorists from entering the United States, particularly from Canada; to enable authorities to detain and deport alien terrorists and those who support them; and to provide humanitarian immigration relief for foreign victims of the attacks on September 11.

Border Protection. The border protection provisions:

- authorize the appropriations necessary to triple the number of Border Patrol, Customs Service, and Immigration and Naturalization Service (INS) personnel stationed along the Northern Border, section 401

- authorize appropriations of an additional $50 million for both INS and the Customers Service to upgrade their border surveillance equipment, section 402

- remove for fiscal year 2001 the $30,000 ceiling on INS overtime pay for border duty, section 404

- authorize appropriations of $2 million for a report to be prepared by the Attorney General on the feasibility of enhancing the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and similar systems to improve the reliability of visa applicant screening, section 405

- authorize the appropriations necessary to provide the State Department and INS with criminal record identification information relating to visa applicants and other applicants for admission to the United States, section 403.

- instruct the Attorney General to report on the feasibility of the use of a biometric identifier scanning system with access to IAFIS for overseas consular posts and points of entry into the United States, section 1007

- direct the Secretary of State to determine whether consular shopping is a problem, to take any necessary corrective action, and to report the action taken, section 418

- express the sense of the Congress that the Administration should implement the integrated entry and exit data system called for by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1365a), section 414

- add the White House Office of Homeland Security to the Integrated Entry and Exit Data System Task Force (8 U.S.C. 1365a note), section 415

- call for the implementation and expansion of the foreign student visa monitoring program (8 U.S.C. 1372), section 416

- limit countries eligible to participate in the visa waiver program to those with machine-readable passports as of October 1, 2003 (8 U.S.C. 1187(c)), section 417

- instruct the Attorney General to report on the feasibility of using biometric scanners to help prevent terrorists and other foreign criminals from entering the country, section 1008[104]

- authorize appropriations of $250,000 for the FBI to determine the feasibility of providing airlines with computer access to the names of suspected terrorists, section 1009

- authorize reciprocal sharing of the State Department's visa lookout data and related information with other nations in order to prevent terrorism, drug trafficking, slave marketing, and gun running, section 413

Detention and Removal. Foreign nationals (aliens) are deportable from the United States, among other grounds, if they were inadmissible at the time they entered the country or if they have subsequently engaged in terrorist activity, 8 U.S.C. 1227 (a)(1)(A), (a)(4)(B), 1182(a)(3)(B)(iv). Aliens may be inadmissible for any number of terrorism-related reasons, 8 U.S.C. 1182 (a)(3)(B). Section 411 of the Act adds to the terrorism-related grounds upon which an alien may be denied admission into the United States and consequently upon which he or she may be deported.

Prior law recognized five terrorism-related categories of inadmissibility. Section 411 redefines two of these – engaging in terrorist activity and representing a terrorist organization (8 U.S.C. 1182(a)(3)(B)(iv), (a)(3)(B)(i)(IV)) – and it adds three more – espousing terrorist activity, being the spouse or child of an inadmissible alien associated with a terrorist organization, and intending to engage in activities that could endanger the welfare, safety or security fo the United States (8 U.S.C. 1182(a)(3)(B)(i)(VI), (a)(3)(B)(i)(VII), 1182(a)(3)(F). It defined engaging in terrorist activity, which is grounds for both inadmissibility and deportation, to encompass soliciting on behalf of a terrorist organization or providing material support to a terrorist organization, 8 U.S.C. 1182(a)(3)(B)(iii)(2000 ed.). It did not explain in so many words, however, what constituted a "terrorist organization," but it presumably included groups designated as terrorist organizations under section 219 of the Immigration and Nationality Act, 8 U.S.C. 1189.

Section 411 defines "terrorist organization" to include not only organizations designated under section 219 but also organizations which the Secretary of State has identified in the *Federal Register* as having provided material support for, committed, incited, planned, or gathered information on potential targets of, terrorist acts of violence, 8 U.S.C. 1182(a)(3)(B)(vi), (a)(3)(B)(iv). It then recasts the definition of engaging in terrorist activities to include solicitation on behalf of such organizations, or recruiting on their behalf, or providing them with material support, 8 U.S.C.

---

[104] As the House Judiciary Committee explained, "A biometric fingerprint scanning system is a sophisticated computer scanning technology that analyzes a person's fingerprint and compares the measurement with a verified sample digitally stored in the system. The accuracy of these systems is claimed to be above 99.9%. The biometric identifier system contemplated by this section would have access to the database of the Federal Bureau of Investigation Integrated Automated Fingerprint Identification System," H.R.Rep.No. 107-236, at 78 (2001).

1182(a)(3)(B)(iv). Nevertheless, section 411 permits the Secretary of State or Attorney General to conclude that the material support prohibition does not apply to particular aliens, 8 U.S.C. 1182(a)(3)(B)(vi).

Prior law made representatives of terrorist organizations designated by the Secretary under section 219 (8 U.S.C. 1189) inadmissible, 8 U.S.C. 1182(a)(3)(B)(i)(IV)(2000 ed.). And so they remain. Section 411 makes representatives of political, social or similar groups, whose public endorsements of terrorist activities undermines U.S. efforts to reduce or eliminate terrorism, inadmissible as well, 8 U.S.C. 1882(a)(3) (B)(i)(IV).

An individual who uses his or her place of prominence to endorse, espouse, or advocate support for terrorist activities or terrorist organizations in a manner which the Secretary of State concludes undermines our efforts to reduce or eliminate terrorism becomes inadmissible under section 411, 8 U.S.C. 1182(a)(3)(B)(i)(VI).

The spouse or child of an alien, who is inadmissible on terrorist grounds for activity occurring within the last 5 years, is likewise inadmissible, unless the child or spouse was reasonably unaware of the disqualifying conduct or has repudiated the disqualifying conduct, 8 U.S.C. 1182(a)(3)(B)(i)(VII), 1182(a)(3)(B)(ii).

Finally, any alien, whom the Secretary of State or the Attorney General conclude has associated with a terrorist organization and intends to engage in conduct dangerous to the welfare, safety, security of the United States while in this country, is inadmissible, 8 U.S.C. 1182(a)(3)(F).

Section 219 of the Immigration and Nationality Act (8 U.S.C. 1189) permits the Secretary to designate as terrorist organizations any foreign group which he finds to have engaged in terrorist activities. A second subsection 411(c) permits him to designate groups which as subnational groups or clandestine agents, engage in "premeditated, politically motivated violence perpetrated against noncombatant targets," or groups which retain the capacity and intent to engage in terrorism or terrorist activity, 8 U.S.C. 1189(a)(1)(B).

Section 412 permits the Attorney General to detain alien terrorist suspects for up to seven days, 8 U.S.C. 1226a. He must certify that he has reasonable grounds to believe that the suspects either are engaged in conduct which threatens the national security of the United States or are inadmissible or deportable on grounds of terrorism, espionage, sabotage, or sedition. Within seven days, the Attorney General must initiate removal or criminal proceedings or release the alien. If the alien is held, the determination must be reexamined every six months to confirm that the alien's release would threaten national security or endanger some individual or the general public. The Attorney General's determinations are subject to review only under writs of habeas corpus issued out of any federal district court but appealable only to the United States Court of Appeals for the District Columbia. The Attorney General must report to the Judiciary Committee on the details of the operation of section 412.

Uncertain is the relationship between section 412 and the President's Military Order of November 13, 2001, which allows the Secretary of Defense to detain designated alien terrorist suspects, within the United States or elsewhere, without

express limitation or condition except with regard to food, water, shelter, clothing, medical treatment, religious exercise, and a proscription on invidious discrimination, 66 *Fed.Reg.* 57833, 57834 (Nov. 16, 2001).

Victims. The Act contains a number of provisions designed to provide immigration relief for foreign nationals, victimized by the attacks of September 11. It provides for:

- permanent resident alien status for eligible aliens and members of their family who but for the events of September 11 would have been eligible for employer-sponsored permanent resident alien status, section 421[105]
- extended filing deadlines for aliens prevented from taking timely action because of immigration office closures, airline schedule disruptions or other similar impediments, section 422[106]

---

[105] "The Act provides permanent resident status through the special immigrant program to an alien who was the beneficiary of a petition filed (on or before September 11) to grant the alien permanent residence as an employer-sponsored immigrant or of an application for labor certification (filed on or before September 11), if the petition or application was rendered null because of the disability of the beneficiary or loss of employment of the beneficiary due to physical damage to, or destruction of, the business of the petitioner or applicant as a direct result of the terrorist attacks on September 11, or because of the death of the petitioner or applicant as a direct result of the terrorist attacks. Permanent residence would be granted to an alien who was the spouse or child of an alien who was the beneficiary of a petition filed on or before September 11 to grant the beneficiary permanent residence as a family-sponsored immigrant (as long as the spouse or child follows to join not later than September 11, 2003). Permanent residence would be granted to the beneficiary of a petition for a nonimmigrant visa as the spouse or the fiancé (and their children) of a U.S. citizen where the petitioning citizen died as a direct result of the terrorist attack. The section also provides permanent resident status to the grandparents of a child both of whose parents died as a result of the terrorist attacks, if either of such deceased parents was a citizen of the U.S. or a permanent resident," H.R.Rep.No. 107-236, at 66-7 (2001).

[106] "The Act provides that an alien who was legally in a nonimmigrant status and was disabled as a direct result of the terrorist attacks on September 11 (and his or her spouse and children) may remain lawfully in the U.S. (and receive work authorization) until the later of the date that his or her status normally terminates or September 11, 2002. Such status is also provided to the nonimmigrant spouse and children of an alien who died as a direct result of the terrorist attacks.

"The Act provides that an alien who was lawfully present as a nonimmigrant at the time of the terrorist attacks will be granted 60 additional days to file an application for extension or change of status if the alien was prevented from so filing as a direct result of the terrorist attacks. Also, an alien who was lawfully present as a nonimmigrant at the time of the attacks but was then unable to timely depart the U.S. as a direct result of the attacks will be considered to have departed legally if doing so before November 11. An alien who was in lawful nonimmigrant status at the time of the attacks (and his or her spouse and children) but not in the U.S. at that time and was then prevented from returning to the U.S. in order to file a timely application for an extension of status as a direct result of the terrorist attacks will be given 60 additional days to file an application and will have his or her status extended 60 days beyond the original due date of the application.

"Under current law, winners of the fiscal year 2001 diversity visa lottery must enter the U.S. or adjust status by September 30, 2001. The Act provides that such an alien may enter

• preservation of certain immigration benefits available to alien family members that would be otherwise lost as a consequence of the death of a victim of September 11, section 423[107]

• limited easing of age restrictions on visas available to aliens under 21 years of age for those whose 21st birthday occurred immediately before or soon after September 11, section 424[108]

• temporary administrative relief for alien family members of a victim of September 11 who are not otherwise entitled to relief under the Act, section 425

---

the U.S. or adjust status until April 1, 2002, if the alien was prevented from doing so by September 30, 2001 as a direct result of the terrorist attacks. If the visa quota for the 2001 diversity visa program has already been exceeded, the alien shall be counted under the 2002 program. Also, if a winner of the 2001 lottery died as a direct result of the terrorist attacks, the spouse and children of the alien shall still be eligible for permanent residence under the program. The ceiling placed on the number of diversity immigrants shall not be exceeded in any case.

"Under the Act, in the case of an alien who was issued an immigrant visa that expires before December 31, 2001, if the alien was unable to timely enter the U.S. as a direct result of the terrorist attacks, the validity shall be extended until December 31.

"Under the Act, in the case of an alien who was granted parole that expired on or after September 11, if the alien was unable to enter the U.S. prior to the expiration date as a direct result of the terrorist attacks, the parole is extended an additional 90 days.

"Under the Act, in the case of an alien granted voluntary departure that expired between September 11 and October 11, 2001, voluntary departure is extended an additional 30 days," H.R.Rep.No. 107-236, at 67-8 (2001).

[107] "Current law provides that an alien who was the spouse of a U.S. citizen for at least 2 years before the citizen died shall remain eligible for immigrant status as an immediate relative. This also applies to the children of the alien. The Act provides that if the citizen died as a direct result of the terrorist attacks, the 2 year requirement is waived.

"The Act provides that if an alien spouse, child, or unmarried adult son or daughter had been the beneficiary of an immigrant visa petition filed by a permanent resident who died as a direct result of the terrorist attacks, the alien will still be eligible for permanent residence. In addition, if an alien spouse, child, or unmarried adult son or daughter of a permanent resident who died as a direct result of the terrorist attacks was present in the U.S. on September 11 but had not yet been petitioned for permanent residence, the alien can self-petition for permanent residence.

"The Act provides that an alien spouse or child of an alien who 1) died as a direct result of the terrorist attacks and 2) was a permanent resident (petitioned-for by an employer) or an applicant for adjustment of status for an employment-based immigrant visa, may have his or her application for adjustment adjudicated despite the death (if the application was filed prior to the death)," H.R.Rep.No. 107-236, at 68 (2001)..

[108] "Under current law, certain visas are only available to an alien until the alien's 21st birthday. The Act provides that an alien whose 21st birthday occurs this September and who is a beneficiary for a petition or application filed on or before September 11 shall be considered to remain a child for 90 days after the alien's 21st birthday. For an alien whose 21st birthday occurs after this September, (and who had a petition for application filed on his or her behalf on or before September 11) the alien shall be considered to remain a child for 45 days after the alien's 21st birthday," H.R.Rep.No. 107-236, at 68 (2001).

• a denial of benefits of the Act to terrorists and their families, section 427

•authority for the Attorney General to establish evidentiary standards to implement the alien victim provisions of the Act, section 426.

Other Crimes, Penalties, & Procedures

New Crimes. The Act creates new federal crimes for terrorist attacks on mass transportation facilities, for biological weapons offenses, for harboring terrorists, for affording terrorists material support, for misconduct associated with money laundering already mentioned, for conducting the affairs of an enterprise which affects interstate or foreign commerce through patterned commission of terrorist offenses, and for fraudulent charitable solicitation. Although strictly speaking these are new federal crimes, they generally supplement existing law filling gaps and increasing penalties.

Pre-existing federal law criminalized, among other things, wrecking trains, 18 U.S.C. 1992, damaging commercial motor vehicles or their facilities, 18 U.S.C. 33, or threatening to do so, 18 U.S.C. 35, destroying vessels within the navigable waters of the United States, 18 U.S.C. 2273, destruction of vehicles or other property used in or used in activities affecting interstate or foreign commerce by fire or explosives, 18 U.S.C. 844(i), possession of a biological agent or toxin as a weapon or a threat, attempt, or conspiracy to do so, 18 U.S.C. 175, use of a weapon of mass destruction affecting interstate or foreign commerce or a threat, attempt, or conspiracy to do so, 18 U.S.C. 2332a, commission of a federal crime of violence while armed with a firearm, or of federal felony while in possession of an explosive, 18 U.S.C. 924(c), 844(h), conspiracy to commit a federal crime, 18 U.S.C. 371.

The Act outlaws terrorist attacks and other actions of violence against mass transportation systems. Offenders may be imprisoned for life or any term of years, if the conveyance is occupied at the time of the offense, or imprisoned for not more than twenty years in other cases, section 801. Under its provisions, it is a crime to willfully:

• wreck, derail, burn, or disable mass transit;
• place a biological agent or destructive device on mass transit recklessly or with the intent to endanger;
• burn or place a biological agent or destructive device in or near a mass transit facility knowing a conveyance is likely to be disabled;
• impair a mass transit signal system;
• interfere with a mass transit dispatcher, operator, or maintenance personnel in the performance of their duties recklessly or with the intent to endanger;
• act with the intent to kill or seriously injure someone on mass transit property;
• convey a false alarm concerning violations of the section;
• attempt to violate the section;
• threaten or conspire to violate the section

when the violation involves interstate travel, communication, or transportation of materials or that involves a carrier engaged in or affecting interstate or foreign commerce, 18 U.S.C. 1993.

Prior to enactment of the Act, federal law proscribed the use of biological agents or toxins as weapons, 18 U.S.C. 175. As suggested by the Justice Department,[109] the Act, in section 817, makes two substantial changes. It makes it a federal offense, punishable by imprisonment for not more than ten years and/or a fine of not more than $250,000, to possess a type or quantity of biological material that cannot be justified for peaceful purposes, 18 U.S.C. 175(b). Second, consistent with federal prohibitions on the possession of firearms, 18 U.S.C. 922(g), and explosives, 18 U.S.C. 842(i), it makes it a federal offenses for certain individuals – such as convicted felons, illegal aliens, and fugitives – to possess biological toxins or agents, 18 U.S.C. 175b.[110] Offenders face the same sanctions, imprisonment for not more than ten years and/or a fine of not more than $250,000.

It is a federal crime to harbor aliens, 8 U.S.C. 1324, or those engaged in espionage, 18 U.S.C. 792; or to commit misprision of a felony (which may take the form of harboring the felon), 18 U.S.C. 4; or to act as an accessory after the fact to a federal crime (including by harboring the offender), 18 U.S.C. 3. The Justice Department had asked that a terrorist harboring offense be added to the espionage section. It also recommended venue and extraterritorial auxiliaries.[111]

---

[109] "Current law prohibits the possession, development, acquisition, etc. of biological agents or toxins for use as a weapon. 18 U.S.C. §175. This section amends the definition of 'for use as a weapon' to include all situations in which it can be proven that the defendant had a purpose other than a prophylactic, protective, or peaceful purpose. This will enhance the government's ability to prosecute suspected terrorists in possession of biological agents or toxins, and conform the scope of the criminal offense in 18 U.S.C. §175 more closely to the related forfeiture provision in 18 U.S.C. §176 [which permits confiscations in cases where the amounts possessed exceed the quantities justifiable for peaceful purposes]. Moreover, the section adds a subsection to 18 U.S.C. §175 which defines an additional offense of possessing a biological agent or toxin of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective or other peaceful purpose. This section also enacts a new statute, 18 U.S.C. 175b, which generally makes it an offense for a person to possess a listed biological agent or toxin if the person is disqualified from firearms possession under 18 U.S.C. §922(g). . . ." *DoJ* at §305.

[110] The section covers those under felony indictment, those convicted of a felony, fugitives, drug addicts, illegal aliens, mental defectives, aliens from countries which support terrorism, and those dishonorably discharged from the U.S. armed forces, 18 U.S.C. 175b(b)(2).

[111] "18 U.S.C. §792 makes it an offense to harbor or conceal persons engaged in espionage. There is no comparable provision for terrorism, though the harboring of terrorists creates a risk to the nation readily comparable to that posed by harboring spies. This section accordingly amends 18 U.S.C. §792 to make the same prohibition apply to harboring or concealing persons engaged in federal terrorism offenses as defined in section 309 of the bill," *DoJ* at §307; *Draft* at §307(2)("There is extraterritorial Federal jurisdiction over any violation (including, without limitation, conspiracy or attempt) of this section. A violation of this section may be prosecuted in any Federal judicial district in which the underlying offense was committed, or in Federal judicial district as provided by law").

The Act, in section 803, instead establishes a separate offense which punishes harboring terrorists by imprisonment for not more than ten years and/or a fine of not more than $250,000, 18 U.S.C. 2339. The predicate offense list consists of:

- destruction of aircraft or their facilities, 18 U.S.C. 32;
- biological weapons offenses, 18 U.S.C. 175;
- chemical weapons offenses, 18 U.S.C. 229;
- nuclear weapons offenses, 18 U.S.C. 831;
- bombing federal buildings, 18 U.S.C. 844(f);
- destruction of an energy facility, 18 U.S.C. 1366;
- violence committed against maritime navigational facilities, 18 U.S.C. 2280;
- offenses involving weapons of mass destruction, 18 U.S.C. 2232a;
- international terrorism, 18 U.S.C. 2232b;
- sabotage of a nuclear facility, 42 U.S.C. 2284;
- air piracy, 49 U.S.C. 46502.

It grants the Justice Department request to permit prosecution either in the place where the harboring occurred or where the underlying act of terrorism committed by the sheltered terrorist might be prosecuted. The Constitution, however, may insist that prosecution take place where the crime of harboring occurred.[112]

Sections 2339A and 2339B of the title 18 of the United States Code ban providing material support to individuals and to organizations that commit various crimes of terrorism. The Act amends the sections in several ways in section 805. Section 2339B (support of a terrorist organization) joins section 2339A (support of a terrorist) as a money laundering predicate offense, 18 U.S.C. 1956(c)(7)(D) The predicate offense list of 18 U.S.C. 2339A (support to terrorists) grows to include:

---

[112] *U.S.Const.* Art.III, §2, cl.3 ("The trial of all crimes . . . shall be held in the state where the said crimes shall have been committed . . . ."); Amend. IV ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed. . . ."); *United States v. Cabrales*, 524 U.S. 1 (1998)(a defendant charged with one count of conspiracy to launder the proceeds of a Missouri drug operation and two counts of laundering in Florida could not be prosecuted in Missouri on the laundering counts). The Court might be thought to have retreated somewhat from *Cabrales* when it later approved prosecution for carrying a firearm in relation to a crime of violence in federal court in New Jersey (where the underlying kidnaping occurred) notwithstanding the fact that the firearm had been acquired in Maryland after the defendants left New Jersey with their victim in tow, *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280-81 n.4 (1999)("By way of comparison, last Term in [*Cabrales*] we considered whether venue for money laundering, in violation of 18 U.S.C. 1956(a)(1)(B) (ii) and 1957, was proper in Missouri, where the laundered proceeds were unlawfully generated, or rather, only in Florida, where the prohibited laundering transactions occurred. As we interpreted the laundering statutes at issue, they did not proscribe the anterior criminal conduct that yielded the funds allegedly laundered. The existence of criminally generated proceeds was a circumstance element of the offense but the proscribed conduct – defendant's money laundering activity – occurred after the fact of an offense begun and completed by others. Here, by contrast, given the 'during and in relation to' language [of section 924], the underlying crime of violence is a critical part of the §924(c)(1) offense").

- chemical weapons offenses, 18 U.S.C. 229;
- terrorist attacks on mass transportation, 18 U.S.C. 1993 ;
- sabotage of a nuclear facility, 42 U.S.C. 2284; and
- sabotage of interstate pipelines, 49 U.S.C. 60123(b).

And it adds expert advice or assistance to the types of assistance that may not be provided under section 2339A. This last addition may encounter the same First Amendment vagueness problems some courts have found in assistance which takes the form of "training" and "personnel," *Humanitarian Law Project v. Reno*, 205 F.3d 1130, 1137-136 (9th Cir. 2000).[113] Finally, the section announces that a prosecution for violation of section 2339A (support of terrorists) may be brought where the support is provided or where the predicate act of terrorism occurs. There may be some question whether the Constitution permits prosecution where the predicate act occurs.[114]

Section 813 of the Act also accepts the Justice Department's suggestion that various terrorism offenses be added to the predicate offense list for RICO (racketeer influenced and corrupt organizations) which proscribes acquiring or operating, through the patterned commission of any of a series of predicate offenses, an enterprise whose activities affect interstate or foreign commerce, 18 U.S.C. 1961.[115]

Prior law, 18 U.S.C. 2325-2327, outlawed violation of Federal Trade Commission (FTC) telemarketing regulations promulgated under 15 U.S.C. 6101 *et seq.* Section 1011 of the Act brings fraudulent charitable solicitations within the FTC's regulatory authority.[116]

---

[113] The Justice Department sought the expansion along with the enlargement of the predicate offense list, "18 U.S.C. §2339A prohibits providing material support or resources to terrorists. The existing definition of 'material support or resources' is generally not broad enough to encompass expert services and assistance – for example, advice provided by a person with expertise in aviation matters to facilitate an aircraft hijacking, or advice provided by an accountant to facilitate the concealment of funds used to support terrorist activities. This section accordingly amends 18 U.S.C. §2339A to include expert services and assistance, making the offense applicable to experts who provide services or assistance knowing or intending that the services or assistance is to be used in preparing for or carrying out terrorism crimes. This section also amends 18 U.S.C. §2339A to conform its coverage of terrorism crimes to the more complete list specified in section 309 of the bill ('Federal terrorism offenses')," *DoJ* at 306.

[114] *U.S.Const.* Art.III, §2, cl.3; Amend. IV; *United States v. Cabrales*, 524 U.S. 1 (1998); *United States v. Rodriguez-Moreno*, 526 U.S. 275 (1999).

[115] "The list of predicate federal offenses for RICO, appearing in 18 U.S.C. §1961(1), includes none of the offenses which are most likely to be committed by terrorists. This section adds terrorism crimes to the list of RICO predicates, so that RICO can be used more frequently in the prosecution of terrorist organizations. As in various other provisions, the list of offenses in section 309 of the bill ('Federal terrorism offenses') is used in identifying the relevant crimes," *DoJ*, at §304.

[116] For a general discussion, *see*, Wellborn, *Combating Charitable Fraud: An Overview of State and Federal Law*, CRS REP.NO. RS21058 (Nov. 7, 2001).

New Penalties. The Act increases the penalties for acts of terrorism and for crimes which terrorists might commit. More specifically it establishes an alternative maximum penalty for acts of terrorism, raises the penalties for conspiracy to commit certain terrorist offenses, envisions sentencing some terrorists to life-long parole, and increases the penalties for counterfeiting, cybercrime, and charity fraud.

The Justice Department suggested an alternative term of imprisonment up to life imprisonment for anyone convicted of an offense designated a terrorist crime. It characterized its proposal as analogous to the standard fine provisions of 18 U.S.C. 3571(b),(c). Section 3571 sets a basic maximum fine of $250,000 for any individual who convicted of a federal felony notwithstanding any lower maximum fine called for in the statute that outlaws the offense.[117]

The proposal, however, failed to identify the critical elements that would trigger the alternative.[118] Both practical and constitutional challenges might be thought to attend this failure to distinguish between those convicted of some "garden variety" crime of terrorism and the more serious offender meriting the alternative, supplementary penalty. Perhaps for this reason, the Act opted to simply increase the maximum penalties for various crimes of terrorism, particularly those which involve the taking of a human life and are not already capital offenses, section 810. Thus, it increases the maximum terms imprisonment for:

- for life-threatening arson or arson of a dwelling committed within a federal enclave, from 20 years to any term of years or life, 18 U.S.C. 81;

- for causing more than $100,000 in damage to, or significantly impairing the operation of an energy facility, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 1366;

---

[117] "Under existing law, the maximum prison terms for federal offenses are normally determined by specifications in the provisions which define them. These provisions can provide inadequate maxima in cases where the offense is aggravated by its terrorist character or motivation. This section accordingly adds a new subsection (e) to 18 U.S.C. §3559 which provides alternative maximum prison terms, including imprisonment for any term of years or for life, for crimes likely to be committed by terrorists. This is analogous to the maximum fine provisions of 18 U.S.C. §3571(b)-(c) – which supersede lower fine amounts specified in the statutes defining particular offenses – and will more consistently ensure the availability of sufficiently high maximum penalties in terrorism cases. As in several other provisions of this bill, the list of the serious crimes most frequently committed by terrorists set forth in section 309 of the bill ('Federal terrorism offenses' is used in defining the scope of the provision,"*DoJ*, at §302.

[118] "A person convicted of any Federal terrorism offense may be sentenced to imprisonment for any term of years or for life, notwithstanding any maximum term of imprisonment specified in the law describing the offense. The authorization of imprisonment under this subsection is supplementary to, and does not limit, the availability of any other penalty authorized by the law describing the offense, including the death penalty, and does not limit the applicability of any mandatory minimum term of imprisonment, including any mandatory life term, provided by the law describing the offense," *Draft* at §302.

• for providing material support to a terrorist or a terrorist organization, from 10 to 15 years (or any term of years or life, if death results), 18 U.S.C. 2339A, 2339B;

• for destruction of national defense materials, from 10 to 20 years (or any term of years or life, if death results), 18 U.S.C. 2155;

• for sabotage of a nuclear facility, from 10 to 20 years (or any term of years or life, if death results), 42 U.S.C. 2284;

• for carrying a weapon or explosive abroad an aircraft with U.S. special aircraft jurisdiction, from 15 to 20 years (or any term of years or life, if death results), *49 U.S.C. 46505; and*

• for sabotage of interstate gas pipeline facilities, from 15 to 20 years (or any term of years or life, if death results), 49 U.S.C. 60123.

It is a separate federal offense punishable by imprisonment for not more than five years to conspire to commit any federal felony, 18 U.S.C. 371. Co-conspirators are likewise subject to punishment for the underlying offense and for any other crimes committed in furtherance of the conspiracy. Nevertheless, some federal criminal statutes impose the same penalties for both the crimes they proscribe and any conspiracy to commit them. The Justice Department urged similar treatment for crimes of terrorism.[119] Again, the Act, in section 811, opts for a less sweeping approach and establishes equivalent sanctions for conspiracy and the underlying offense in cases of:

• arson committed within a federal enclave, 18 U.S.C. 81;
• killing committed while armed with a firearm in a federal building, 18 U.S.C. 930(c);
• destruction of communications facilities, 18 U.S.C. 1362;
• destruction of property within a federal enclave, 18 U.S.C. 1363;
• causing a train wreck, 18 U.S.C. 1922;
• providing material support to a terrorist, 18 U.S.C. 2339A;
• torture committed overseas under color of law, 18 U.S.C. 2340A;
• sabotage of a nuclear facility, 42 U.S.C. 2284;

---

[119] "The maximum penalty under the general conspiracy provision of federal criminal law (18 U.S.C. §371) is five years, even if the object of the conspiracy is a serious crime carrying a far higher maximum penalty. For some individual offenses and types of offense, special provisions authorize conspiracy penalties equal to the penalties for the object offense – see e.g., 21 U.S.C. §846 (drug crimes) – but there is no consistently applicable provision of this type for the crimes that are likely to be committed by terrorists.

"This section accordingly adds a new §2332c to the terrorism chapter of the criminal code – parallel to the drug crime conspiracy provision in 21 U.S.C. §846 – which provides maximum penalties for conspiracies to commit terrorism crimes that are equal to the maximum penalties authorized for the objects of such conspiracies. This will more consistently provide adequate penalties for terrorist conspiracies. As in various other provisions of this bill, the relevant class of offenses is specified by the notion of 'Federal terrorism offense,' which is defined in section 309 of the bill," *DoJ* at §303.

- interfering with a flight crew within U.S. special aircraft jurisdiction, 49 U.S.C. 46504;
- carrying a weapon or explosive abroad an aircraft within U.S. special aircraft jurisdiction, 49 U.S.C. 46505; and
- sabotage of interstate gas pipeline facilities, 49 U.S.C. 60123.

When federal courts impose a sentence of a year or more upon a convicted defendant, they must also impose a term of supervised release, 18 U.S.C. 3583; U.S.S.G. §5D1.1. Supervised release is not unlike parole, except that it is ordinarily imposed in addition to (rather than in lieu of) a term, or portion of a term, of imprisonment. The term may be no longer than 5 years for most crimes and violations of the conditions of release may result in imprisonment for up to an additional 5 years, 18 U.S.C. 3583(e). The terms of supervisory release for drug dealers, however, are often cast as mandatory minimums with no statutory ceiling. Thus, for example, a dealer convicted of distributing more than a kilogram of heroin must receive a term of supervised release of "at least 5 years" in addition to a term of imprisonment imposed for the offense, 21 U.S.C. 841(b). Although a majority feel that the more specific drug provisions of 21 U.S.C. 841 trump the more general limitations of 18 U.S.C. 3583, some of the federal appellate courts believe the two should be read in concert where possible (*e.g.*, at least but not more than 5 years).[120] The Justice Department recommended a maximum supervisory term of life for those convicted of acts of terrorism (subject to the calibrations of the Sentencing Commission),[121] a recommendation which the Act accepted in section 812 but only in the case of terrorists whose crimes resulted in death or were marked by a foreseeable risk of death or serious bodily injury, 18 U.S.C. 3583(j).

---

[120] *Compare, United States v. Barragan*, 263 F.3d 919, 925-26 (9th Cir. 2001); *United States v. Pratt*, 239 F.3d 640, 646-48 (4th Cir. 2001); *United States v. Heckard*, 238 F.3d 1222, 1237 (10th Cir. 2001); and *United States v. Aguayo-Delgado*, 220 F.3d 926, 933 (8th Cir. 2000); *with, United States v. Meshack*,2 25 F.3d 556, 578 (5th Cir. 2001); and *United States v. Samour*, 199 F.3d 821, 824-25 (6th Cir. 2001).

[121] "Existing federal law (18 U.S.C. 3583(b)) generally caps the maximum period of post-imprisonment supervision for released felons at 3 or 5 years. Thus, in relation to a released but still unreformed terrorist, there is no means of tracking the person or imposing conditions to prevent renewed involvement in terrorist activities beyond a period of a few years. The drug laws (21 U.S.C. §841) mandate longer supervision periods for persons convicted of certain drug trafficking crimes, and specify no upper limit on the duration of supervision, but there is nothing comparable for terrorism offenses.

"This section accordingly adds a new subsection to 18 U.S.C. 3583 to authorize longer supervision periods, including potentially lifetime supervision, for persons convicted of terrorism crimes. This would permit appropriate tracking and oversight following release of offenders whose involvement with terrorism may reflect lifelong ideological commitments. As in other provisions in this bill, the covered class of crimes is federal terrorism offenses, which are specified in section 390 of the bill.

"This section affects only the maximum periods of post-release supervision allowed by statute. It does not limit the authority of the Sentencing Commission and the courts to tailor the supervision periods imposed in particular cases to offense and offender characteristics, and the courts will retain their normal authority under 18 U.S.C. §3583(e)(1) to terminate supervision if it is no longer warranted," *DoJ* at §308.

Sometime ago, Congress outlawed computer fraud and abuse (cybercrime) involving "federal protected computers" (*i.e.*, those owned or used by the federal government or by a financial institution or used in interstate or foreign commerce), 18 U.S.C. 1030. Section 814 of the Act increases the penalty for intentionally damaging a protected computer from imprisonment for not more than 5 years to imprisonment for not more than 10 years (from not more than 10 to not more than 20 years for repeat offenders).[122]

Finally, section 1011 increases the penalty for fraudulently impersonating a Red Cross member or agent (18 U.S.C. 917) from imprisonment for not more than 1 year to imprisonment for not more than 5 years.

Other Procedural Adjustments. In other procedural adjustments designed to facilitate criminal investigations, the Act:

- increases the rewards for information in terrorism cases
- expands the Posse Comitatus Act exceptions
- authorizes "sneak and peek" search warrants
- permits nationwide and perhaps worldwide execution of warrants in terrorism cases
- eases government access to confidential information
- allows the Attorney General to collect DNA samples from prisoners convicted of any crime of violence or terrorism
- lengthens the statute of limitations applicable to crimes of terrorism
- clarifies the application of federal criminal law on American installations and in residences of U.S. government personnel overseas
- adjusts federal victims' compensation and assistance programs

A section found in the Senate bill, but ultimately dropped, would have changed the provision of law that required Justice Department prosecutors to adhere to the ethical standards of the legal profession where they conduct their activities (the McDade-Murtha Amendment), 28 U.S.C. 530B.[123]

---

[122] It provides a comparable increase to not more than 20 years (from not more than 10 years) for those who recklessly damage a protected computer following a prior computer abuse conviction. Civil and criminal liability for simply causing protected computer damage (as opposed to intentionally or reckless causing the damage) is limited to special circumstances, *e.g.*, damage in excess of $5000, damage causing physical injury, etc.; section 814 adds to the list of circumstances upon which liability may be predicated. To the list of predicate circumstances, it adds causing damage to a computer used by the government for the administration of justice, national defense, or national security.

[123] When presenting the final bill to the House, the Chairman of the Judiciary Committee noted, "the Senate bill contained revisions of the so-called McDade law. This compromise version does not contain those changes, and I agreed to review this subject in a different context," 147 *Cong.Rec.* H7196 (daily ed. Oct. 23, 2001)(remarks of Rep. Sensenbrenner); for general background, *see*, Doyle, *McDade-Murtha Amendment: Ethical Standards for Justice Department Attorneys*, CRS REP.NO. RL30060 (Dec. 14, 2001).

Rewards. The Attorney General already enjoys the power to pay rewards in criminal cases, but his powers under other authorities is often subject to caps on the amount he might pay. Thus as a general rule, he may award amounts up to $25,000 for the capture of federal offenders, 18 U.S.C. 3059, and may pay rewards in any amount in recognition of assistance to the Department of Justice as long as the Appropriations and Judiciary Committees are notified of any rewards in excess of $100,000, 18 U.S.C. 3059B. Although he has special reward authority in terrorism cases, individual awards were capped at $500,000, the ceiling for the total amount paid in such rewards was $5 million, and rewards of $100,000 or more required his personal approval or that of the President, 18 U.S.C. 3071-3077. Over the last several years, annual appropriation acts have raised the $500,000 cap to $2 million and the $5 million ceiling to $10 million, *e.g.*, P.L. 106-553, 114 Stat. 2762-67 (2000); P.L. 106-113, 113 Stat. 1501A-19 (1999); P.L.105-277, 112 Stat. 2681-66 (1998).

The Act supplies the Attorney General with the power to pay rewards to combat terrorism in any amount and without an aggregate limitation, but for rewards of $250,000 or more it insists on personal approval of the Attorney General or the President and on notification of the Appropriations and Judiciary Committees, section 501 (18 U.S.C. 3071). In addition, the counterterrorism fund of section 101 can be used "without limitation" to pay rewards to prevent, investigate, or prosecute terrorism.[124]

The Secretary of State's reward authority was already somewhat more generous than that of the Attorney General. He may pay rewards of up to $5 million for information in international terrorism cases as long as he personally approves payments in excess $100,000, 22 U.S.C. 2708. The Act removes the $5 million cap and allows rewards to be paid for information concerning the whereabouts of terrorist leaders and facilitating the dissolution of terrorist organizations, section 502.

Posse Comitatus. The Posse Comitatus Act and its administrative auxiliaries, 18 U.S.C. 1385, 10 U.S.C. 375, ban use of the armed forces to execute civilian law, absent explicit statutory permission. One existing statutory exception covers Department of Justice requests for technical assistance in connection with emergencies involving biological, chemical or nuclear weapons, 18 U.S.C. 2332e, 10 U.S.C. 382. The Act enlarges the exception to include emergencies involving other weapons of mass destruction, section 104.[125]

Delayed notification of a search (sneak and peek). Rule 41 of the Federal Rules of Criminal Procedure seemed to preclude "sneak and peek" warrants before passage of the Act. A sneak and peek warrant is one that authorizes officers to secretly enter, either physically or virtually; conduct a search, observe, take

---

[124] The fund is otherwise available to reestablish capacity lost in terrorist attacks, to conduct threat assessments for federal agencies, and to reimburse federal agencies for the costs of detaining terrorist suspects overseas.

[125] For a general discussion of the Posse Comitatus Act, *see*, Doyle, *The Posse Comitatus Act & Related Matters: The Use of the Military to Execute Civilian Law*, CRS REP.NO. 95-964 (June 1, 2000).

measurements, conduct examinations, smell, take pictures, copy documents, download or transmit computer files, and the like; and depart without taking any tangible evidence or leaving notice of their presence. The Rule required that after the execution of a federal search warrant officers leave a copy of the warrant and an inventory of what they have seized (tangible or intangible), and they were to advise the issuing court what they had done, F.R.Crim.P. 41(d). To what extent did Rule 41 portray the standards for a reasonable search and seizure for purposes of the Fourth Amendment?

The Fourth Amendment clearly requires officers to knock and announce their purpose before entering to execute a warrant, *Richards v. Wisconsin*, 520 U.S. 385 (1997), but with equal clarity recognizes exceptions for exigent circumstances such as where compliance will lead to the destruction of evidence, flight of a suspect, or endanger the officers, *Wilson v. Arkansas*, 514 U.S. 927 (1995). It is undisputed that Title III (the federal wiretap statute) is not constitutionally invalid because it permits delayed notice of the installation of an interception device, *Dalia v. United States*, 441 U.S. 238 (1979). Finally, there is no doubt that the Fourth Amendment imposes no demands where it does not apply. Thus, chapter 121 (court authorization for disclosure of the contents of e-mail stored with third party service providers) may permit delayed notification of the search of e-mail in remote storage with a third party for more than 180 days without offending the Fourth Amendment, because there is no Fourth Amendment justifiable expectation of privacy under such circumstances, *cf., United States v. Miller*, 425 U.S. 435 (1976).

The lower federal courts are divided over the extent to which the Rule reflects Fourth Amendment requirements. The Ninth Circuit saw the Fourth Amendment reflected in Rule 41, *United States v. Freitas*, 800 F.2d 1451, 1453 (9th Cir. 1986).[126]

---

[126] "The district court held that a search warrant permitting agents to observe, but not seize tangible property was impermissible under Rule 41. That holding conflicts with language in *United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977): Although Rule 41(h) defines property to include documents, books, papers, and any other tangible objects, it does not restrict or purport to exhaustively enumerate all the items which may be seized pursuant to Rule 41. . . . Rule 41 is not limited to tangible items. That case held seizures of intangibles were not precluded by the definition of property appearing in Rule 41(b). Without doubt there was a search in this case. Its purpose, we hold, was to seize intangible, not tangible, property. The intangible property to be seized was information regarding the status of the suspected clandestine methamphetamine laboratory. The search was authorized by a warrant supported by what the district court concluded was probable cause. . . . The question remains, however, whether a warrant lacking both a description of the property to be seized and a notice requirement conforms to Rule 41. . . . we hold that there was no compliance with Rule 41 under the facts of this case. . . . While it is clear that the Fourth Amendment does not prohibit all surreptitious entries, it is also clear that the absence of any notice requirement in the warrant casts strong doubt on its constitutional adequacy. We resolve those doubts by holding that in this case the warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed seven days except upon a strong showing of necessity. We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interests, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth

The Second Circuit was less convinced and preferred to hold sneak and peek searches to the demands of Rule 41, *United States v. Pangburn*, 983 F.2d 449 (2d Cir. 1993).[127] The Fourth Circuit was, if anything, less convinced. Moreover, the facts in the case demonstrate the potential impact of the issue on computer privacy, *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).[128]

Amendment, demands that surreptitious entries be closely circumscribed," *United States v. Freitas (Freitas I)*, 800 F.2d 1451, 1455-456 (9th Cir. 1986). The court remanded the case for a determination of whether grounds existed for a good faith exception to application of the exclusionary rule. It subsequently declined to exclude the evidence on those grounds, *United States v. Freitas (Freitas II)*, 856 F.2d 1425 (9th Cir. 1988).

[127] "No provision specifically requiring notice of the execution of a search warrant is included in the Fourth Amendment. Accordingly, in *Dalia v. United States*, 441 U.S. 238, 247 (1979), the Supreme Court found no basis for a constitutional rule proscribing all covert entries. Resolving the particular issue raised in *Dalia,* the Court determined that the Fourth Amendment does not prohibit per se a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment. Rule 41 of the Federal Rules of Criminal Procedure does require notice of the execution of a search warrant but does not prescribe when the notice must be given. Rule 41 by its terms provides for notice only in the case of seizures of physical property. . . . The Supreme Court also has held that the authority conferred by Rule 41 is not limited to the seizure of tangible items. *See United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977). Despite the absence of notice requirements in the Constitution and Rule 41, it stands to reason that notice of a surreptitious search must be given at some point after the covert entry. . . .Although the *Freitas I* court specifically determined that the warrant was constitutionally defective for failure to include a notice requirement, we made no such determination in *United States v. Villegas*, 899 F.2d 1324 (1999). Although the *Freitas I* court found that covert entry searches without physical seizure strike at the very heart of the Fourth Amendment-protected interests, we used no such language in *Villegas*. Indeed, it was our perception that a covert entry search for intangibles is less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property. . . . We prefer to root out notice requirement in the provisions of Rule 41 rather than in the somewhat amorphous Fourth Amendment interests concept developed by the *Freitas I* court. The Fourth Amendment does not deal with notice of any kind, but Rule 41 does. It is from the Rule's requirements for service of a copy of the warrant and for provision of an inventory that we derive the requirements of notice in cases where a search warrant authorizes covert entry to search and to seize intangibles," *United States v. Pangburn*, 983 F.2d 449, 453-55 (2d Cir. 1993).

[128] In *Simons*, a search team entered Simons' office at night in his absence and "copied the contents of Simons' computer; computer diskettes found in Simons' desk drawer; computer files stored on the zip drive or on zip drives diskettes; videotapes; and various documents, including personal correspondence. No original evidence was removed from the office. Neither a copy of the warrant nor a receipt for the property seized was left in the office or otherwise given to Simons at that time, and Simons did not learn of the search for approximately 45 days." A property list, however, was returned to the magistrate. In the view of the Fourth Circuit, "[t]here are two categories of Rule 41 violations; those involving constitutional violations and all others. The violations termed 'ministerial' in our prior cases obviously fall into the latter category. Nonconstitutional violations of Rule 41 warrant suppression only when the defendant is prejudiced by the violation, or when there is evidence of intentional and deliberate disregard of a provision in the Rule. First, we conclude that the failure of the team executing the warrant to leave either a copy of the warrant or a receipt for the items taken did not render the search unreasonable under the Fourth Amendment. The

The Justice Department urged that the conflict be resolved with a uniform rule which permitted sneak and peek warrants under the same circumstances that excused delayed notification of government access to e-mail to longer-term, remote, third party storage.[129]

The Act, in section 213, stops short of the Justice Department proposal. Characterized as a codification of the Second Circuit decision, 147 *Cong.Rec.* H7197 (daily ed. Oct. 23, 2001), the Act extends the delayed notification procedure of chapter 121, which operates in an area to which the Fourth Amendment is inapplicable, to cases to which the Fourth Amendment applies, 18 U.S.C. 3103a. Its sneak and peek authorization reaches all federal search and seizure warrants where the court finds reasonable cause to believe that notification would have the kind of adverse results depicted in 18 U.S.C. 2705. Section 2705 describes both exigent circumstances (*e.g.*, risk of destruction of evidence or bodily injury) and circumstances that are not likely to excuse notification when it is required by the Fourth Amendment (*e.g.*, jeopardizing an investigation; delaying a trial). The sneak and peek authorization, however, does not reach tangible evidence, or wire or electronic communication unless the court finds the seizure "reasonably necessary." It is not clear whether reasonable necessity means a seizure necessary to the investigation that is also reasonable in a Fourth Amendment sense, *i.e.*, in the presence of exigent circumstances, or whether it means a seizure which a reasonable judge might find necessary for the investigation.[130] The doctrine of constitutional avoidance argues against the latter interpretation. By the same token, when the Act permits delay for a reasonable period, it should probably be understood to mean

---

Fourth Amendment does not mention notice, and the Supreme Court has stated that the constitution does not categorically proscribe covert entries, which necessarily involve a delay in notice. And insofar as the August search satisfied the requirements of the Fourth Amendment, *i.e.*, it was conducted pursuant to a warrant based on probable cause issued by a neutral and detached magistrate, we perceive no basis for concluding that the 45-day delay in notice rendered the search unconstitutional. Having concluded that the Rule 41(d) violation at issue here did not infringe on Simons' constitutional rights, we must now evaluate his argument that the violation was deliberate. . . . The district court did not address the intent issue when it ruled on Simons' motion to suppress. . . . We therefore remand for the district court to consider whether the Government intentionally and deliberately disregarded the notice provision of Rule 41(d) when it carried out the August 6, 1998 search," 206 F.3d at 403.

[129] "The law that currently governs notice to subjects of warrants where there is a showing to the court that immediate notice would jeopardize an ongoing investigation or otherwise interfere with lawful law enforcement activities, is a mix of inconsistent rules, practices, and court decisions varying widely from jurisdiction to jurisdiction across the country. This greatly hinders the investigation of many terrorism cases and other cases. This section resolves this problem by establishing a statutory, uniform standard for all such circumstances. It incorporates by reference the familiar, court-enforced standards currently applicable to stored communications under 18 U.S.C. §2705, and applies them to all instances where the court is satisfied that immediate notice of execution of a search warrant would jeopardize an ongoing investigation or otherwise interfere with lawful law-enforcement activities," *DoJ* at §353.

[130] Since neither the restriction nor its reasonable necessity exception appeared in the Justice Department's initial proposal, the Department's justification does not address the question.

constitutionally "reasonable," that is, a brief period reasonable in light of the exigent circumstances which allow the delay or their like.

Nationwide terrorism search warrants. The Fourth Amendment demands that warrants be issued by a neutral magistrate, *Coolidge v. New Hampshire*, 403 U.S. 443 (1971); the Sixth Amendment, that crimes be prosecuted in the districts where they occur, *United States v. Cabrales*, 524 U.S. 1 (1998). The Federal Rules direct magistrates to issue warrants only for property within their judicial district, although they permit execution outside the district for property located in the district when the warrant is sought but removed before execution can be had, F.R.Crim.P. 41(a).

The Act, in section 219, allows a magistrate in the district in which a crime of terrorism has occurred to issue a search warrant to be executed either "within or outside the district," (F.R.Crim.P. 41(a)(3)) in domestic and international terrorism cases.[131] The provision may anticipate execution both in this country and overseas.[132] The Fourth Amendment does not apply to the overseas searches of the property of foreign nationals, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). It does apply to the search of American property overseas involving American authorities, although the lower federal courts are divided over the exact level of participation required to trigger coverage.[133] Neither Rule 41 nor any other provision of federal

---

[131] The amended rule uses the definitions of domestic and international terrorism found in 18 U.S.C. 2331, as modified by section 802 of the Act: "(1) the term 'international terrorism' means activities that – (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum . . . (5) the term 'domestic terrorism' means activities that – (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended – (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States," 18 U.S.C. 2331(1),(5).

[132] The Justice Department, with whom the proposal originated, was somewhat cryptic on this point. Its analysis suggests execution in one of the several judicial districts of the United States, but not so precisely as to negate any other construction. "The restrictiveness of the existing rule creates unnecessary delays and burdens for the government in the investigation of terrorist activities and networks that span a number of districts, since warrants must be separately obtained in each district. This section resolves that problem by providing that warrants can be obtained in any district in which activities related to the terrorism may have occurred, regardless of where the warrants will be executed," *DoJ* at §351.

[133] *United States v. Barona*, 56 F.3d 1087, 1092 (9th Cir. 1995)("United States agents' participation in the investigation is so substantial that the action is a joint venture between United States and foreign officials"); *United States v. Behety*, 32 F.3d 503, 510 (11th Cir. 1994)("if American law enforcement officials substantially participated in the search or if the

law apparently contemplated extraterritorial execution, *cf.,* F.R.Crim.P.41, *Advisory Committee Notes: 1990 Amendment* (discussing a proposal for extraterritorial execution that the Supreme Court rejected). [134]

If the Act anticipates overseas execution there may be some question whether it creates a procedure to be used in lieu of extradition when the person for whom the search warrant has been issued is located outside the United States. The section refers to warrants for "search of property *or for a person* within or outside the district," §219 (emphasis added). The Judicial Conference in 1990 recommended an amendment to Rule 41, which the Supreme Court rejected, that would have permitted the overseas execution of federal search warrants. In doing so, the Conference suggested extraterritorial execution be limited to warrants to search for property and not reach warrants to search for persons, *"lest the rule be read as a substitute for* extradition proceedings," F.R.Crim.P. 41, *Advisory Committee Notes: 1990 Amendment.* There is no indication, however, that the section is at odds with either the Fourth or Sixth Amendment.

Terrorists' DNA. The courts have generally concluded that the collection of DNA information from convicted prisoners does not offend constitutional standards *per se.* [135] Existing federal law allowed the Attorney General to collect samples from

---

foreign officials conducting the search were actually acting as agents for their American counterparts"); *United States v. Maturo*, 982 F.2d 57, 61 (2d Cir. 1992)("where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials" or "where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional requirements applicable to American officials"); *United States v. Mitro*, 880 F.2d 1480, 1482 (1st Cir. 1989)("where American agents participated in the foreign search or the foreign officers acted as agents for their American counterparts"); *United States v. Mount*, 757 F.2d 1315, 1318 (D.C.Cir. 1985)("if American officials or officers participated in some significant way"); *United States v. Marzano*, 537 F.2d 257, 270 (7th Cir. 1976)(declining to adopt the "joint venture" standards, but finding level of American participation in the case before it insignificant); *United States v. Morrow*,5 37 F.2d 120, 139 (5th Cir. 1976)("if American law enforcement officials participated in the foreign search, or if the foreign authorities actually conducting the search were acting as agents for their American counterparts"); each of the decisions also suggests that evidence secured in a manner which shocked the conscience of the court would be excluded.

[134] The Code still carries remnants of the consular courts which speak of the overseas execution of arrest warrants in places where the United States has "extraterritorial jurisdiction," 18 U.S.C. 3042. The history of the provisions makes it clear that the phrase "extraterritorial jurisdiction" was intended to coincide with those places in which the U.S. had consular courts, *see*, S.Rep. 217, 73d Cong., 2d Sess. 3 (1934), *reprinted*, 78 *Cong.Rec.* 4982-983 (1934)("The countries to which the proposed bill, if enacted into law, would relate are the following, in which the United States exercises extraterritorial jurisdiction: China, Egypt, Ethiopia, Muscat, and Morocco"); 22 U.S.C. 141 (1926 ed.)(conferring judicial powers on consular courts there identified as those located in China, Egypt, Ethiopia, Muscat, Morocco, Siam and Turkey).

[135] *Roe v. Marcotte*,1 93 F.3d 72 (2d Cir. 1999); *Shaffer v. Saffle*, 148 F.3d 1180 (10th Cir. 1998); *Rise v. Oregon*, 59 F.3d 1556 (9th Cir. 1995); *Jones v. Murray*, 962 F.2d 302 (4th Cir. 1992).

federal prisoners convicted of a variety of violent crimes, 42 U.S.C. 14135a. The Act enlarges the predicate offense list to include any crime of violence or any terrorism offense, section 503.[136]

Access to Educational Records. Finally, the Act calls for an ex parte court order procedure under which senior Justice Department officials may seek authorization to collect educational records relevant to an investigation or prosecution of a crime of terrorism, section 507 (as an exception to the confidentiality requirements of the General Education Provisions Act, 20 U.S.C. 1232g), section 508 (as an exception to the confidentiality requirements of the National Education Statistics Act, 20 U.S.C. 9007).

Statute of Limitations. Prosecution for murder in violation of federal law may be initiated at any time, 18 U.S.C. 3281. A five year statute of limitations applied for most other federal crimes before passage of the Act, with a few exceptions. Among the relevant exceptions were an eight year statute of limitations for several terrorist offenses, 18 U.S.C. 3286,[137] and a ten year statute of limitations for a few arson and explosives offenses, 18 U.S.C. 3295. The Justice Department recommended the elimination of a statute of limitations in terrorism cases.[138]

---

[136] Summarizing the law in place at the time, the Department of Justice argued that, "The statutory provisions governing the collection of DNA samples form convicted federal offenders (42 U.S.C. §14135a(d)) are restrictive, and do not include persons convicted for the crimes that are most likely to be committed by terrorists. DNA samples cannot now be collected even from persons federally convicted of terrorist murders in most circumstances. For example, 49 U.S.C. §46502, which applies to terrorists who murder people by hijacking aircraft, 18 U.S.C. §844(i), which applies to terrorists who murder people by blowing up buildings, and 18 U.S.C. 2332, which applies to terrorists who murder U.S. nationals abroad, are not included in the qualifying federal offenses for purposes of DNA sample collection under existing law. This section addresses the deficiency of the current law in relation to terrorists by extending DNA sample collection to all persons convicted of terrorism crimes," *DoJ* at §353.

For a general discussion, *see*, Fischer, *DNA Identification: Applications and Issues*, CRS REP.NO. RL30717 (Jan. 12, 2001).

[137] 18 U.S.C. 32 (destruction of aircraft or aircraft facilities), 37 (violence at international airports), 112 (assaults on foreign dignitaries), 351 (crimes of violence against Members of Congress), 1116 (killing foreign dignitaries), 1203 (hostage taking), 1361 (destruction of federal property), 1751 (crimes of violence against the President), 2280 (violence against maritime navigation), 2281 (violence on maritime platforms), 2332 (terrorist violence against Americans overseas), 2332a (use of weapons of mass destruction), 2332b (acts of terrorism transcending national boundaries), 2340A (torture); 49 U.S.C. 46502 (air piracy), 46504 (interference with a flight crew), 46505 (carrying a weapon aboard an aircraft), and 46506 (assault, theft, robbery, sexual abuse, murder, manslaughter or attempted murder or manslaughter in the special aircraft jurisdiction of the United States).

[138] "This section amends 18 U.S.C. §3286 to provide that terrorism of offenses may be prosecuted without limitation of time. This will make it possible to prosecute the perpetrators of terrorist acts whenever they are identified and apprehended.

"This section expressly provides that it is applicable to offenses committed before the date of enactment of the statute, as well as those committed thereafter. This retroactivity provision ensures that no limitation period will bar the prosecution of crimes committed in

The Act takes less dramatic action in section 809. It eliminates the statute of limitations for any crime of terrorism[139] that risks or results in a death or serious bodily injury, 18 U.S.C. 3286. In the absence of such a risk or result, all other terrorism offenses become subject to the eight year statute of limitations unless already covered by the ten year statute for explosives and arson offenses, 18 U.S.C. 3286.

Application of the statute of limitations rarely provokes a constitutional inquiry. Nevertheless, due process precludes prosecution when it can be shown that pre-indictment delay "caused substantial prejudice to [a defendant's] rights to a fair trial and that the delay was an intentional device to gain tactical advantage over the accused."[140] Moreover, a judicial difference of opinion has appeared in those cases

---

connection with the September 11, 2001 terrorist attacks. The constitutionality of such retroactive applications of changes in statutes of limitations is well-settled, See, e.g., *United States v. Grimes*, 142 F.3d 1342, 1350-51 (11th Cir. 1998); *People v. Frazer*, 982 P.2d 180 (Cal. 1999).

"Existing federal law (18 U.S.C. §3282) bars prosecuting most offenses after five years. 18 U.S.C. §3286, as currently formulated, extends the limitation period for prosecution for certain offenses that may be committed by terrorists – but only to eight years. While this is a limited improvement over the five-year limitation period for most federal offenses, it is patently inadequate in relation to the catastrophic human and social costs that frequently follow from such crimes as destruction of aircraft (18 U.S.C. §32), aircraft hijackings ([49] U.S.C. §§46502, 46504-06, attempted political assassinations (18 U.S.C. §§351, 1116, 1751), or hostage taking (18 U.S.C. §1203). These are not minor acts of misconduct which can properly be forgiven or forgotten merely because the perpetrator has avoided apprehension for some period of time. Anomalously, existing law provides longer limitation periods for such offenses as bank frauds and certain artwork thefts (18 U.S.C.§§3293-94) than it does for crimes characteristically committed by terrorists.

"In many American jurisdictions, the limitation periods for prosecution for serious offenses are more permissible than those found in federal law, including a number of states which have no limitation period for the prosecution of felonies generally. While this section does not go so far, it does eliminate the limitation period for prosecution of the major crimes that are most likely to be committed by terrorists ('Federal terrorism offenses'), as specified in section 309 of this bill," *DoJ* at 301.

[139] As defined by 18 U.S.C. 2332b(g)(5)(B), with the amendments of §808, this includes, in addition to the offenses already listed in 18 U.S.C. 3296 – 18 U.S.C. 81 (arson within U.S. special maritime and territorial jurisdiction); 175 & 175b (biological weapons); 229 (chemical weapons); 831 (nuclear weapons); 842(m) & (n) (plastic explosives); 844(f)(bombing federal property where death results); 844(i)(bombing property used in interstate commerce); 930(c)(possession of a firearm in a federal building where death results), 956(a)(conspiracy within the U.S. to commit murder, kidnapping, or to maim overseas); 1030(a) (1), (5)(A)(i), (5)(B)(ii)-(v)(computer abuse); 1114 (killing federal officers or employees); 1362 (destruction of communications facilities); 1363 (malicious mischief within the U.S. special maritime and territorial jurisdiction); 1366(a)(destruction of an energy facility); 1992 (train wrecking); 1993 (terrorist attack on mass transit); 2155 (destruction of national defense materials); 2339 (harboring terrorists); 2339A (material support to terrorists), 2339B (material support to terrorist organizations); 42 U.S.C. 2284 (sabotage of nuclear facilities); and 49 U.S.C. 60123(b)(destruction of pipeline facilities).

[140] *United States v. Marion*, 404 U.S. 307, 325 (1971); *United States v. Lovasco*, 431 U.S. 783,790 (1977).

when an existing period of limitation is enlarged legislatively and the new period made applicable to past offenses. The lower federal courts have long noted that the Constitution poses no impediment to enlarging a period of limitation *as long as it does not revive an expired period.*[141] Recently, however, the California Supreme Court held that retroactive revival of an expired statute of limitations offended neither the California nor the United States Constitution.[142]

Section 809 applies "to the prosecution of any offense committed before, on, or after the date of enactment of this section," the very words used in the Justice Department proposal. The Justice Department, in describing its proposal, cited both federal law (*Grimes*, where the court held that extensions may be applied where the earlier period of limitations has not expired) and California law (*Frazer*, where the court held that extensions may revive an expired period of limitations). The implication is that the Justice Department understood its proposal to apply to past offenses whether the earlier statute of limitations had expired or not. Other than its use of identical terminology, Congress gave no hint of whether it intended to adopt this view for section 809. Whether the federal courts could be persuaded to overcome their previously expressed constitutional reservations is equally uncertain.

Extraterritoriality. Crime is usually outlawed, prosecuted and punished where it is committed. In the case of the United States, this is ordinarily a matter of practical and diplomatic preference rather than constitutional necessity. Consequently, although prosecutions are somewhat uncommon, a surprising number of federal criminal laws have extraterritorial application. In some instances, the statute proscribing the misconduct expressly permits the exercise of extraterritorial jurisdiction, 18 U.S.C. 2381 (treason) ("Whoever, owing allegiance to the United States . . . within the United States or elsewhere. . ."). In others, such as those banning assassination of Members of Congress, 18 U.S.C. 351, or the murder of federal law enforcement officers, 18 U.S.C. 1114, the courts have assumed Congress intended the prohibitions to have extraterritorial reach.[143]

The Act touches upon extraterritoriality only to a limited extent and in somewhat unusual ways. Congress has made most common law crimes – murder, sexual abuse, kidnaping, assault, robbery, theft and the like – federal crimes when committed within the special maritime and territorial jurisdiction of the United States. The special maritime and territorial jurisdiction of the United States represents two variations of extraterritorial jurisdiction.

---

[141] *United States v. De La Matta*, 266 F.3d 1275, 1286 (11th Cir. 2001); *United States v. Grimes*, 142 F.3d 1342, 1351 (11th Cir. 1998); *United States v. Morrow*, 177 F.3d 272, 294 (5th Cir. 1999); *Falter v. United States*, 23 F.2d 420, 425-26 (2d Cir. 1928).

[142] *People v. Frazer*, 24 Cal.4th 737, 759, 982 P.2d 180, 1294, 88 Cal.Rptr.2d 312, 327 (1999).

[143] *United States v. Layton*, 855 F.2d 1388 (9th Cir. 1988)(at the time of the overseas murder of Congressman Ryan for which Layton was convicted the statute was silent as to its extraterritorial application; several years later Congress added an explicit extraterritorial provision, 18 U.S.C. 351(i)); *United States v. Benitez*, 741 F.2d 1312 (11th Cir. 1984)(18 U.S.C. 1114 has since expanded to protect all federal officers and employees, including members of the armed forces and those assisting them).

The special maritime jurisdiction of the United States extends to the vessels of United States registry. Historically, the territorial jurisdiction of the United States was thought to reach those areas over which Congress enjoyed state-like legislative jurisdiction. For some time, those territories were located exclusively within the confines of the United States, but over the years they came to include at least temporarily, Hawaii, the Philippines, and several other American overseas territories and possessions. Recently, the lower federal courts have become divided over the question of whether laws, enacted to apply on federal enclaves within the United States and within American territories overseas, might also apply to areas in foreign countries over which the United States has proprietary control.[144]

The Act resolves the conflict by declaring within the territory of the United States those overseas areas used by American governmental entities for their activities or residences for their personnel, at least to the extent that crimes are committed by or against an American, section 804 (18 U.S.C. 7 (9)). The section is inapplicable where it would otherwise conflict with a treaty obligation or where the offender is covered by the Military Extraterritorial Jurisdiction Act, 18 U.S.C. 3261.

Victims. Federal law has provided for crime victim compensation and assistance programs for some time. Moreover, Congress enacted September 11th Victim Compensation Fund legislation before it passed the Act. Consequently, the Act's victim provisions focus on adjustments to existing programs, primarily to those of the Victims of Crime Act of 1984, 42 U.S.C. 10601 *et seq.*, and to those maintained for the benefit of public safety officers and their survivors, 42 U.S.C. 3796 *et seq.*

Public safety officers - police officers, firefighters, ambulance and rescue personnel - killed or disabled in the line of duty (and their heirs) are entitled to federal benefits. Prior to the Act, death benefits were set at $100,000 and the total amount available for disability benefits in a given year was capped at $5 million, 42 U.S.C. 3796 (2000 ed.). No benefits could be paid for suicides, if the officer was drunk or grossly negligent, if the beneficiary contributed to the officer's death or injury, or if the officer were employed other than in a civilian capacity, 42 U.S.C. 3796 (2000 ed.). The Act increases the death benefit to $250,000 (retroactive to January 1, 2001), section 613; and for deaths and disability connected with acts of terrorism waives the $5 million disability cap and the disqualifications for gross negligence, contributing cause, or employment in a noncivilian capacity, section 611.

Most of fines collected for violation of federal criminal laws are deposited in the Crime Victims Fund which is available for child abuse prevention and treatment grants, victim services within the federal criminal justice system, and grants to state victim compensation and victim assistance programs, 42 U.S.C. 10601 to 10608. The Act:

---

[144] *Compare, United States v. Gatlin*, 216 F.3d 207 (2d Cir. 2000); *United States v. Laden*, 92 F.Supp.2d 189 (S.D.N.Y. 2000); *with, United States v. Corey*, 232 F.3d 1166 (9th Cir. 2000); *United States v. Erdos*, 474 F.2d 157 (4th Cir. 1973).

• authorizes private contributions to the fund (42 U.S.C. 10601(b)), section 621(a)

• instructs the Department of Justice, which administers the fund, to distribute in every fiscal year (if amounts in the Fund are sufficient) amounts equal to between 90% and 110% of the amount distributed in the previous fiscal year (120% in any year when the amount on hand is twice the amount distributed the previous year)(42 U.S.C. 10601(c)), section 621(b)

• reduces by 1% the amounts available for compensation and assistance grants (from 48.5% to 47.5% after child abuse and federal victim priorities have been met), and increases from 3% to 5% the amount available for Justice Department discretionary spending for demonstration projects and services to assist the victims of federal crimes (42 U.S.C. 10601(d), 10603(c)), section 621(c)

• converts the general reserve fund to an antiterrorism reserve fund and reduces the cap on the reserve from $100 million to $50 million (42 U.S.C. 10601(d)(5)), section 621(d)

• waives the Fund's availability caps with respect to funds transferred to it in response to the terrorist attacks of September 11 (42 U.S.C. 10601 note)), section 621(e)

• lowers the annual reduction rate on individual compensation program grants; beginning in 2003 individual grants are limited to 60% (rather than 40%) of the amount of awarded in the previous year (42 U.S.C. 10602(a)), section 622(a)

• eliminates the requirement that state compensation programs permit compensation for state residents who are the victims of terrorism overseas (42 U.S.C. 10602(b)(6)(B)), section 622(b)

• provides that compensation under the September 11th Victim Compensation Fund should be counted as income in considering eligibility for any federal indigent benefit program (42 U.S.C. 10602(c)), section 622(c)

• drops "crimes involving terrorism" from the definition of "compensable crime"; it is unclear whether the phrase was removed as redundant or pursuant to a determination to compensate victims other than through the Crime Victims Fund (42 U.S.C. 10602(d)), section 622(d)(1)

• makes it clear that the Virgin Islands is eligible to receive grants (42 U.S.C. 10602(d)), section 622(d)(2)

• adds the September 11th Victim Compensation Fund to the "double dipping" restriction that applies to the victim compensation programs and confirms that state compensation programs will not be rendered ineligible for grants by virtue of a refusal to pay dual compensation to September 11th Fund victims (42 U.S.C. 10602(e)), section 622(e)

• makes federal agencies performing law enforcement functions in the District of Columbia, Puerto Rico, the Virgin Islands, and other U.S. territories and possessions eligible for victim assistance grants (42 U.S.C. 10603(a)(6)), section 623(a)

• prohibits program discrimination against crime victims based on their disagreement with the manner in which the state is prosecuting the underlying offense (42 U.S.C. 10603(b)(1)(F)), section 623(b)

• allows Justice Department discretionary grants for purposes of program evaluation and compliance and for fellowships, clinical internships and training programs (42 U.S.C. 10603(c)(1)(A), (3)(E)), section 623(c),(e)

• reverses the preference for victim service grants over demonstration projects and training grants, so that *not more* than 50% of the amounts available for crime victim assistance grants shall be used for victim service grants and *not less* than 50% for demonstration projects and training grants (42 U.S.C. 10603(c)(2)), section 623(d)

• makes federal and local agencies and private entities eligible for supplemental grants for services relating to victims of terrorism committed within the U.S. (42 U.S.C. 10603b(b)), section 624(a)

• allows supplemental grants for services relating to victims of terrorism committed overseas regardless of whether the victims are eligible for compensation under Title VIII of the Omnibus Diplomatic Security and Antiterrorism Act (100 Stat. 879 (1986))(Title VIII victims were previously ineligible) (42 U.S.C. 10603b(a)(1)), section 624(b)

• establishes a "double dipping" restriction under which compensation to the victims of overseas terrorism is reduced by the amount received under Title VIII of the Omnibus Act (42 U.S.C. 10603c(b)), section 624(c)

Increasing Institutional Capacity. A major portion of the Act is devoted to bolstering the institutional capacity of federal law enforcement agencies to combat terrorism and other criminal threats. In addition to the counterterrorism discussed above in the context of the Attorney General's reward prerogatives, it increases funding authorization for an FBI technical support center, section 103, and allows the FBI to hire translators without regard to otherwise applicable employment restrictions such as citizenship, section 205.

In the area of cybercrime, the Attorney General is instructed to establish regional forensic laboratories, section 817, and the Secret Service, to establish a national network of electronic crime task forces, modeled after its New York Electronic Crimes Task Force, section 105. The Act likewise clarifies the Secret Service's investigative jurisdiction with respect to computer crime (18 U.S.C. 1030) and to crimes involving credit cards, PIN numbers, computer passwords, or any frauds against financial institutions (18 U.S.C. 3056), section 506.

For a period of up to 180 days after the end of Operation Enduring Freedom, section 1010 allows the Department of Defense (DoD) to contract with state and local law enforcement authorities to perform various security functions on its military installations and facilities, 10 U.S.C. 2465.

The Act also authorizes appropriations for wide range anti-terrorism purposes including:

- $25 million a year for FY 2003 through FY 2007 for state and local terrorism prevention and antiterrorism training grants for first responders, section 1005 (28 U.S.C. 509 note)

- necessary sums (FY 2002 through FY 2007) for Office of Justice Programs (OJP) grants to state and local governments to enhance their capacity to respond to terrorist attacks, section 1014 (42 U.S.C. 3711)

- $250 million a year (FY 2002 through FY 2007) for OJP grants to state and local governments integrated information and identification systems, section 1015 (42 U.S.C. 14601)

- $50 million per fiscal year for the Attorney General to develop and support regional computer forensic laboratories (28 U.S.C. 509 note), section 816

- $50 million (FY 2002) and $100 million (FY 2003) for Bureau of Justice Assistance grants (42 U.S.C. 3796h) for federal-state-local law enforcement information sharing systems, section 701

- $20 million (FY 2002) for the activities of National Infrastructure Simulation and Analysis Center in DoD's Defense Threat Reduction Agency, section 1016 (42 U.S.C. 5195c)

- $5 million for DEA police training in South and Central Asia, section 1007.

Miscellaneous. Finally, the Act addresses the issuance of licenses for the drivers of vehicles carrying hazardous materials and the use of trade sanctions against countries that support terrorism.

The Act requires background checks for criminal records and immigration status of applicants for licenses to operate vehicles carrying hazardous materials including chemical and biological materials (49 U.S.C. 5101a), section 1012.

The Trade Sanctions Reform and Export Enhancement Act, 22 U.S.C. 7201 to 7209, limits the President's authority to unilaterally impose export restrictions on food and medical supplies. The limitations do not apply to restrictions on products that might be used for the development or production of chemical or biological weapons or of weapons of mass destruction, 22 U.S.C. 7203(2)(c). The Act expands the exception to include products that might to used for the *design* of chemical or biological weapons or of weapons of mass destruction as well, section 221(a)(1).

Only one year licenses may be issued for trade with countries that sponsor terrorism, 22 U.S.C. 7205. The Act brings areas of Afghanistan controlled by the Taliban within the same restriction, section 221(a)(2).

Neither of these changes or anything else in the trade sanctions legislation precludes the assessment of civil or criminal liability for violations of 18 U.S.C. 2339A (providing support to terrorists), of 18 U.S.C. 2339B (providing support to terrorist organizations), or of various presidential orders under the International Emergency Economic Powers Act,[145] or of restrictions on foreign involvement in weapons of mass destruction or missile proliferation, sections 221(b), 807.[146]

---

[145] *I.e.*, Executive Order No. 12947, 50 U.S.C. 1701 note (prohibiting transactions with terrorists); Executive Order No. 13224, 50 U.S.C. 1701 note (blocking property of persons who support terrorism); Executive Order No. 12978, 50 U.S.C. 1701 note (blocking assets of significant narcotics traffickers).

[146] For a general discussion of trade sanctions legislation, *see,* Jurenas, *Exempting Food and Agriculture Products from U.S. Economic Sanctions: Status and Implementation*, CRS ISSUE BRIEF IB100061.

September 9, 2003

Honorable Patrick J. Leahy
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Leahy:

I am writing in response to your letter to Director Mueller dated July 25, 2003 regarding information on the FBI's website relating to access to library records under Section 215 of the USA PATRIOT Act.

After receiving your letter, we reviewed the portion of the website about which you raised concerns. In doing so, we identified an error relating to the standard of proof for obtaining an order from the Foreign Intelligence Surveillance Court. We have deleted the statement that:

> the FBI must prove to a judge that it has probable cause and must certify to the court that these records are sought for an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

We replaced that language with the statement that:

> the FBI must certify that these records are relevant for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

1 - Mr. Wainstein
1 - Ms. Chandler
1 - Ms. Caproni
1 - Mr. Rowan
1 - Mr. Bowman
[redacted]
1 - Ms. Kalisch
1 - OCA Member's Folder
1 - Exec Sec
EPK:crm(10)

b6
b7C

Rowan, J Patrick

From: [redacted]
Sent: Wednesday, September 10, 2003 2:16 PM
To: Rowan, J Patrick
Cc: KALISCH, ELENI P. [redacted]
Subject: SSCI Member Briefing on 09/11/2003 @ 2:30 p.m.: Patriot Act

b6
b7C

Pat,

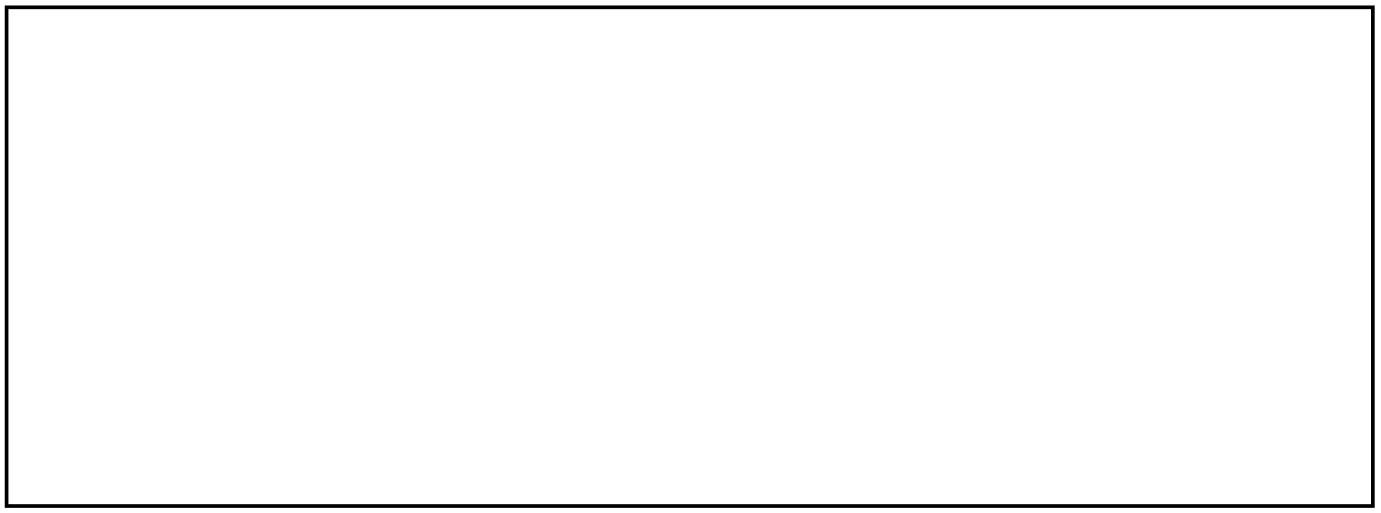
I attended the Pre-Brief at DOJ and provide the following in summary:

[redacted]

b6
b7C
b5

****

[redacted]



b2
b6
b7C
b5

Section 215 of the USA PATRIOT Act

"The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."

House Judiciary Committee ***press release,***
October 17, 2002

50 U.S.C. § 1861. Access to certain business records for foreign intelligence and international terrorism investigations.

(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) Each application under this section

(1) shall be made to—

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in

Comparable to Grand Jury Power: For years, grand juries have issued subpoenas to all types of entities, including libraries and bookstores.

- In a recent **domestic-terrorism** case, a grand jury served a subpoena to a bookseller to obtain records showing that a suspect had purchased a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.
- In the **Gianni Versace** murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.
- In the **Zodiac gunman** investigation, a New York grand jury subpoenaed records from a Manhattan library. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.

First Amendment Rights: Section 215 goes to great lengths to preserve the First Amendment rights of those who are under investigation, including the patrons of libraries and bookstores. FBI agents are prohibited from using a suspect's exercise of First Amendment rights as a pretext for seeking records or information.

Narrow Scope: Section 215 can only be used in a narrow set of investigations: (1) to obtain foreign intelligence information about people who are neither American citizens nor lawful permanent residents; or (2) to defend the United States against spies or international terrorists. Section 215 cannot be used to investigate garden-variety crimes, or even domestic terrorism.

Court Order Requirement: FBI agents cannot obtain records under section 215 unless they receive a court order. Agents cannot use this authority unilaterally to compel libraries or any other entity to turn over their records. They can obtain such documents only by appearing before the FISA court and convincing it that they need them.

subsection (a).

(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

50 U.S.C. § 1862. Congressional oversight.

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 1861 of this title.

(b) On a semiannual basis, the attorney general shall provide to the committees on the judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—

(1) the total number of applications made for orders approving requests for the production of tangible things under section 1861 of this title; and

(2) the total number of such orders either granted, modified, or denied.

Confidentiality Comparable to Other Laws: The requirement that recipients of court orders keep them confidential is based on the "national security letter" statutes, which have existed for decades. (An NSL is a type of administrative subpoena used in certain national-security investigations.)

- 12 U.S.C. § 3414(a)(5)(D): "No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under this paragraph."
- 18 U.S.C. § 2709(c): "No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."

Oversight: Section 215 provides for thorough congressional oversight. Every six months, the Attorney General is required to "fully inform" Congress on the number of times agents have sought a court order under section 215, as well as the number of times such requests were granted, modified, or denied.

Rowan, J Patrick

From: [redacted] b6 b7C
Sent: Thursday, July 10, 2003 11:58 AM
To: Rowan, J Patrick; Rosenberg, Charles P
Subject: RE: Libraries

[redacted] b5

-----Original Message-----
From: Rowan, J Patrick b6
Sent: Thursday, July 10, 2003 10:59 AM
To: [redacted] Rosenberg, Charles P b7C
Subject: RE: Libraries

[redacted]

-----Original Message----- b5
From: [redacted] b5 b6
Sent: Thursday, July 10, 2003 10:52 AM b6 b7C
To: Rosenberg, Charles P; Rowan, J Patrick
Subject: RE: Libraries b7C

Chuck & Pat,

[redacted]

b5

[redacted]

Hope this helps.

[redacted] b5 b6

-----Original Message-----
From: Rosenberg, Charles P
Sent: Thursday, July 10, 2003 5:51 AM
To: Rowan, J Patrick
Cc: [redacted]
Subject: RE: Libraries

b5 b6 b7C

[redacted]

-----Original Message-----
From: Rowan, J Patrick
Sent: Wednesday, July 09, 2003 6:09 PM
To: Rosenberg, Charles P
Subject: RE: Libraries

[redacted]

-----Original Message-----
From: Rosenberg, Charles P
Sent: Wednesday, July 09, 2003 5:17 PM
To: Rowan, J Patrick
Cc: Wainstein, Kenneth L
Subject: Libraries

b5 b6 b7C

Pat: [redacted]

[redacted]

Section 215 of the USA PATRIOT Act

"The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."

House Judiciary Committee ***press release,*** *October 17, 2002*

SEC. 215. ACCESS TO RECORDS AND OTHER ITEMS UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

"SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

"(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.
"(2) An investigation conducted under this section shall—
"(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
"(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

"(b) Each application under this section—
"(1) shall be made to—
"(A) a judge of the court established by section 103(a); or
"(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and
"(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

"(c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.
"(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

Comparable to Grand Jury Power: For years, grand juries have issued subpoenas to all types of entities, including libraries and bookstores.

- In a recent **domestic-terrorism** case, a grand jury served a subpoena to a bookseller to obtain records showing that a suspect had purchased a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.
- In the **Gianni Versace** murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.
- In the **Zodiac gunman** investigation, a New York grand jury subpoenaed records from a Manhattan library. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.

First Amendment Rights: Section 215 goes to great lengths to preserve the First Amendment rights of those who are under investigation, including the patrons of libraries and bookstores. FBI agents are prohibited from using a suspect's exercise of First Amendment rights as a pretext for seeking records or information.

Narrow Scope: Section 215 can only be used in a narrow set of investigations: (1) to obtain foreign intelligence information about people who are neither American citizens nor lawful permanent residents; or (2) to defend the United States against spies or international terrorists. Section 215 cannot be used to investigate garden-variety crimes, or even domestic terrorism.

Court Order Requirement: FBI agents cannot obtain records under section 215 unless they receive a court order. Agents cannot use this authority unilaterally to compel libraries or any other entity to turn over their records. They can obtain such documents only by appearing before the FISA court and convincing it that they need them.

"(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

"(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

"SEC. 502. CONGRESSIONAL OVERSIGHT.

"(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.

"(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period—
"(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and
"(2) the total number of such orders either granted, modified, or denied.".

Confidentiality Comparable to Other Laws: The requirement that recipients of court orders keep them confidential is based on the "national security letter" statutes, which have existed for decades. (An NSL is a type of administrative subpoena used in certain national-security investigations.)

- 12 U.S.C. § 3414(a)(5)(D): "No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under this paragraph."
- 18 U.S.C. § 2709(c): "No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."

Oversight: Section 215 provides for thorough congressional oversight. Every six months, the Attorney General is required to "fully inform" Congress on the number of times agents have sought a court order under section 215, as well as the number of times such requests were granted, modified, or denied.

United States District Court
Eastern District of Michigan

Summons in a Civil Action and Return of Service Form

DENISE PAGE HOOD

MAGISTRATE JUDGE R. STEVEN WHALEN

03-72913
Case Number and Judge Assignment (to be supplied by the Court)

Plaintiff(s) Name		Defendant(s) Name
MUSLIM COMMUNITY ASSOCIATION OF ANN ARBOR, et al. (SEE ATTACHMENT FOR REMAINDER OF PLAINTIFFS)	vs.	JOHN ASHCROFT, in his official capacity as Attorney General of the United States; ROBERT MUELLER, in his official capacity as Director of the Federal Bureau of Investigation,
Plaintiffs attorney, address and telephone:		Name and address of defendant being served:
Ann Beeson/Jameel Jaffer, ACLU Foundation,125 Broad Street, 18th Floor, New York, NY 10004-2400, (212) 549-2500; Michael J. Steinberg, Noel Saleh, Kary L. Moss, ACLU of Michigan, 60 W. Hancock, Detroit, MI 48201; (313)-578-6800		ROBERT MUELLER, Director Federal Bureau of Investigation 935 Pennsylvania Ave., NW Washington, D.C. 20535

To the defendant

This summons is notification that YOU ARE BEING SUED by the above named plaintiff(s).

1. You are required to serve upon the plaintiff's attorney, name and address above, an answer to the complaint within 60 days after receiving this summons, or take other actions that are permitted by the Federal Rules of Civil Procedure.

2. You must file the original and one copy of your answer within the time limits specified above with the Clerk of Court.

3. Failure to answer or take other action permitted by the Federal Rules of Civil Procedure may result in the issuance of a judgment by default against you for the relief demanded in the complaint.

David J. Weaver
Clerk of the Court

By: _____ Deputy Clerk

b6
b7C

For Your Info.
From
Pat Kelley

JUL 30 2003
Date of issuance

INT-0131-MIE-REV. 12/93 06/99

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

MUSLIM COMMUNITY ASSOCIATION OF ANN ARBOR; AMERICAN-ARAB ANTI-DISCRIMINATION COMMITTEE; ARAB COMMUNITY CENTER FOR ECONOMIC AND SOCIAL SERVICES; BRIDGE REFUGEE & SPONSORSHIP SERVICES, INC.; COUNCIL ON AMERICAN-ISLAMIC RELATIONS; ISLAMIC CENTER OF PORTLAND, MASJED AS-SABER,

Plaintiffs,

v.

JOHN ASHCROFT, in his official capacity as Attorney General of the United States; ROBERT MUELLER, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

03-72913

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

DENISE PAGE HOOD

Case No.

MAGISTRATE JUDGE R. STEVEN WHALE
Hon.

ANN BEESON
JAMEEL JAFFER
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500

MICHAEL J. STEINBERG
NOEL SALEH
KARY L. MOSS
American Civil Liberties Union Fund of Michigan
60 West Hancock
Detroit, MI 48201-1343
(313) 578-6800

Attorneys for Plaintiffs

COMPLAINT

PRELIMINARY STATEMENT

1. This lawsuit challenges the constitutionality of Section 215 of the USA PATRIOT Act, which vastly expands the power of the Federal Bureau of Investigation ("FBI") to obtain records and other "tangible things" of people not suspected of criminal activity. Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) ("Patriot Act" or "Act"). The FBI can use Section 215 to obtain personal belongings, including "books, records, papers, documents, and other items," directly from a person's home. It can also order charities, political organizations, libraries, hospitals, Internet Service Providers, or indeed *any* person or entity to turn over the records or personal belongings of others. The FBI can use Section 215 against anyone at all, including United States citizens and permanent residents.

2. Section 215 is invalid on its face. To obtain a Section 215 order, the FBI need only assert that the records or personal belongings are "sought for" an ongoing foreign intelligence, counterintelligence, or international terrorism investigation. The FBI is not required to show probable cause – or any reason – to believe that the target of the order is a criminal suspect or foreign agent. The FBI can obtain and execute Section 215 orders in total secrecy. The targets of Section 215 orders are *never* notified that their privacy has been compromised – even years later, and even if they are innocent. The law includes a gag provision that prohibits persons or entities served with Section 215 orders from ever disclosing, even in the most general terms, that the FBI has sought information from them. By seriously compromising the rights to privacy, free speech, and due process, Section 215 violates the First, Fourth, and Fifth Amendments of the United

States Constitution. Plaintiffs respectfully seek a declaration that Section 215 is facially unconstitutional, and a permanent injunction against its enforcement.

JURISDICTION AND VENUE

3. This case arises under the United States Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the United States Constitution and 28 U.S.C. § 1331. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*. The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412. Venue is proper in this district under 28 U.S.C. § 1391(e).

PARTIES

4. Plaintiff Muslim Community Association of Ann Arbor ("MCA") is a non-profit, membership-based organization that serves the religious needs of Muslims in and around Ann Arbor, Michigan. MCA owns and administers a mosque and an Islamic school. MCA sues on its own behalf and on behalf of its members, students, and constituents.

5. Plaintiff American-Arab Anti-Discrimination Committee ("ADC") is a non-profit civil rights organization committed to defending the rights of people of Arab descent and promoting their rich cultural heritage. ADC, which is non-sectarian and non-partisan, is the largest Arab-American grassroots organization in the United States. Based in Washington, D.C., it was founded in 1980 by former United States Senator James Abourezk and has chapters nationwide. ADC sues on its own behalf and on behalf of its members and constituents.

6. Plaintiff Arab Community Center for Economic and Social Services ("ACCESS") is a Detroit-based human services organization committed to the development of the Arab-American community in all aspects of its economic and cultural life. Among other services, ACCESS operates a Community Health and Research Center. ACCESS sues on its own behalf and on behalf of its members, clients, and constituents.

7. Plaintiff Bridge Refugee & Sponsorship Services, Inc. ("Bridge") is an ecumenical, non-profit organization based in Knoxville, Tennessee, dedicated to helping refugees and asylum-seekers become and stay self-sufficient. Bridge is affiliated with Church World Service and with Episcopal Migration Ministries. Bridge recruits and trains church sponsors to help refugees create new lives in East Tennessee, and provides services until refugees are eligible to apply for United States citizenship. Bridge sues on its own behalf and on behalf of its clients.

8. Plaintiff Council on American Islamic Relations ("CAIR") is a non-profit, mainstream, grassroots organization dedicated to enhancing the public's understanding of Islam and Muslims. CAIR is the largest Islamic civil liberties organization in the United States. CAIR is based in Washington, D.C., and has chapters nationwide and in Canada. CAIR sues on its own behalf and on behalf of its members and constituents.

9. Plaintiff Islamic Center of Portland, Masjed As-Saber ("ICPMA"), is a non-profit organization that serves the religious needs of Muslims in and around Portland, Oregon. ICPMA owns and administers a mosque known as Masjed As-Saber and an Islamic school known as the Islamic School of Portland. ICPMA sues on its own behalf and on behalf of its community members and students.

10. Defendant Attorney General John Ashcroft heads the United States Department of Justice, which is the agency of the United States government responsible for enforcement of federal criminal laws and domestic intelligence investigations. Defendant Attorney General Ashcroft has ultimate authority for supervising all of the operations and functions of the Department of Justice. The Department of Justice includes the FBI, the agency authorized to use the law challenged in this case.

11. Defendant Robert Mueller is the Director of the FBI, which is the principal investigative arm of the United States Department of Justice. Defendant Robert Mueller is responsible for supervising all of the operations and functions of the FBI. The FBI is the agency authorized to use the law challenged in this case.

STATUTORY LANGUAGE AT ISSUE

12. The Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, was enacted in 1978 to govern FBI surveillance of foreign powers and their agents inside the United States. *See* Pub. L. 95-511, 92 Stat. 1783 (Oct. 25, 1978). Through FISA, Congress created the Foreign Intelligence Surveillance Court ("FISA Court"), originally composed of seven (now eleven) federal district judges empowered to grant or deny government applications for FISA surveillance orders. *See* 50 U.S.C. § 1803.

13. Since 1978, Congress has amended FISA numerous times, each time adding new tools to the FBI's foreign intelligence toolbox or expanding the class of investigations in which such tools may be employed.

14. One amendment, which was codified as Subchapter IV of FISA, authorized the FBI to obtain "business records" from vehicle rental agencies, common carriers, storage facilities, and other similar businesses if the FBI had "specific and

articulable facts" giving reason to believe that the records in question pertained to a foreign agent or power. *See* Pub. L. 105-272, Title VI, § 602, 112 Stat. 2411 (Oct. 20, 1998).

15. The Patriot Act was passed on October 26, 2001.

16. Section 215 of the Patriot Act amended Subchapter IV of FISA by: (i) allowing the FBI to demand the production of "any tangible things (including books, records, papers, documents, and other items)," and not just business records; (ii) allowing the FBI to demand books, records and other tangible things from *anyone*, and not just from vehicle rental agencies and other third parties; and (iii) allowing the FBI to demand books, records and other tangible things without showing any evidence that the person whom it is investigating is a foreign agent. *See* 50 U.S.C. § 1861(a)(1).

17. Section 215 does not require the FBI to show probable cause or any reason to believe that the records or personal belongings sought pertain to a person involved in criminal activity or to a foreign agent or foreign power. *See id.* § 1861(b)(2). The provision requires only that the FBI certify to the FISA Court that the books, records, or other tangible things demanded on the authority of the provision are "sought for" a foreign intelligence, clandestine intelligence, or international terrorism investigation. As a result of the changes effected by the Patriot Act, the FBI is now authorized to use Section 215 even against people who are known to be altogether unconnected to criminal activity or espionage.

18. Section 215 requires the FISA Court to defer to the FBI's specification that the records or personal belongings sought by a Section 215 order are sought for an investigation to obtain foreign intelligence information or to protect against international

terrorism or clandestine intelligence activities. The FISA Court has no statutory authority to examine the foundation of the FBI's specification or to reject the specification as unfounded. *See id.* § 1861(b)(2) & (c)(1).

19. Section 215 does not require the FBI to have reason to believe that the records or personal belongings sought pertain to a particular suspect or a particular offense. Accordingly, the FBI could use Section 215 to obtain from a bookstore a list of people who had purchased a particular book, or to obtain from a health clinic a list of patients who had received medical care. The FBI need not state or even know in advance which individuals' privacy will be infringed.

20. At a hearing before the House Judiciary Committee on June 5, 2003, Defendant Attorney General John Ashcroft stated that, prior to the Patriot Act, the government "used to have [to allege] a reason to believe that the target is an agent of a foreign power," a standard he agreed was "lower than probable cause." He acknowledged that, under Section 215, the government may now obtain "all relevant, tangible items" without such a showing.

21. Section 215 does not require the FBI ever to notify surveillance targets that it has obtained their records or personal belongings.

22. Section 215 does not include any procedure that would allow a person or entity served with a Section 215 order to challenge the order's constitutionality before turning over the records or personal belongings sought by the order.

23. Section 215 authorizes the FBI to obtain records or personal belongings of United States citizens and permanent residents based in part on "activities protected by the first amendment to the Constitution." *Id.* § 1861(a)(1); *see also* § 1861(a)(2)(B).

24. Section 215 authorizes the FBI to obtain records or personal belongings of people who are not United States citizens or permanent residents based *solely* upon "activities protected by the First Amendment to the Constitution." *See id.* § 1861(a)(1); *see also* § 1861(a)(2)(B).

25. Section 215 requires the FISA Court to defer to the FBI's specification that the investigation is not being conducted of a United States person solely upon the basis of activities protected by the First Amendment. The FISA Court has no statutory authority to examine the foundation of the FBI's specification or to reject the specification as unfounded. *See id.* § 1861(b)(2) & (c)(1).

26. Section 215 includes the following gag provision: "No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section." *See id.* § 1861(d). Section 215 gag orders are indefinite, and do not require the FBI to make a showing that secrecy is necessary in any particular case.

27. Defendant Attorney General John Ashcroft has refused to disclose publicly even the most basic information about the FBI's use of Section 215. He has refused to say, for example, how many times the provision has been used to obtain information from public libraries, how many times it has been used to obtain information about United States citizens or permanent residents, and how many times it has been used in response to a person's engagement in activity protected by the First Amendment.

28. Through a request submitted under the Freedom of Information Act, the American Civil Liberties Union obtained heavily redacted documents that indicate that the FBI has already used Section 215.

29. At a June 2003 hearing, Defendant Attorney General Ashcroft informed the House Judiciary Committee that it is his position that Section 215 could be used to obtain, among other things, library and bookstore records, computer files, education records, and even genetic information.

FACTUAL BACKGROUND

30. Based on their personal experiences and the government's own actions, plaintiffs have a well-founded belief that they and their members, clients, and constituents (hereinafter "members and clients") have been or are currently the targets of investigations conducted under Section 215. Because Section 215 does not require the government to provide notice to surveillance targets, and because it strictly gags recipients from disclosing that the FBI has sought or obtained information from them, plaintiffs and other innocent targets of FBI surveillance have no way to know with certainty that their privacy has been compromised.

31. The FBI has already targeted plaintiffs, their members, and their clients in a number of ways.

32. The FBI has sought information directly from some of the plaintiffs about their members and clients.

33. The FBI has sought information from some of the plaintiffs' members and clients directly, either during visits to their homes and businesses, or through numerous

registration and interview programs directed at Muslims of Arab and South Asian descent.

34. Plaintiffs have many members and clients who were required to register under the National Security Entry-Exit Registration System (NSEERS), an INS program that thus far has been applied almost exclusively to nationals of predominantly Arab and Muslim countries. Many individuals who appeared in good faith for registration were then detained by the INS for alleged immigration violations. The FBI also interviewed many of plaintiffs' members and clients of Arab, Muslim, and South Asian descent in March 2002. Finally, the FBI interviewed many of plaintiffs' members and clients of Iraqi descent in March 2003, as part of "Operation Liberty Shield."

35. During these interviews, many members were questioned about their religious and political beliefs, activities, and associations. Some of plaintiffs' members expressed opposition to the war in Iraq, to United States support for Israeli policies, and to other aspects of United States foreign policy. Plaintiffs' members and clients believe that the FBI may have selected them for investigation under Section 215 because of information obtained during these interviews.

36. The Attorney General stated publicly in November 2002 that the Justice Department had a "previously undisclosed intelligence program involv[ing] tracking thousands of Iraqi citizens and Iraqi-Americans with dual citizenship."

37. The FBI is currently investigating a number of charities suspected of providing material support to Foreign Terrorist Organizations. Some of plaintiffs' members and clients contributed financially to these charities before the charities were accused of having provided material support.

38. Some of the plaintiffs and their members and clients have direct contacts with people whom the INS detained and the FBI interrogated after September 11th. The FBI routinely interrogated INS detainees, asking questions not only about the detainees' own immigration status, political views, religious beliefs, and foreign connections but also about the political views, religious beliefs, and foreign connections of the detainees' friends and family members.

39. Many of plaintiffs' members and clients emigrated to the United States from countries the government has accused of sponsoring terrorism, such as Syria and Iraq. Defendant Mueller has stated publicly that a "substantial" number of persons are under constant surveillance, particularly in communities like New York and Detroit, where plaintiffs have thousands of Arab-American members and clients.

40. Many of the plaintiffs directly serve Muslim communities, or have significant numbers of members or clients who are Muslim. Two of the plaintiffs, the Muslim Community Association of Ann Arbor and the Islamic Center of Portland, Masjed As-Saber, operate mosques.

41. Section 215 has caused some of plaintiffs' members and clients to be inhibited from publicly expressing their political views, attending mosque and practicing their religion, participating in public debate, engaging in political activity, associating with legitimate political and religious organizations, donating money to legitimate charitable organizations, exercising candor in private conversations, researching sensitive political and religious topics, visiting particular websites, and otherwise engaging in activity that is protected by the First Amendment to the United States Constitution.

Muslim Community Association of Ann Arbor

42. MCA is a non-profit, membership-based organization that owns and administers a mosque and an Islamic school, the Michigan Islamic Academy, in Ann Arbor, Michigan. Approximately 1000 people attend services at the mosque each Friday; as many as 2500 attend services on religious holidays. MCA employs approximately 20 people and has about 700 registered, dues-paying members.

43. Approximately 200 students are enrolled at the Michigan Islamic Academy, which offers classes from pre-K through 11th grade. In addition to offering the standard academic curriculum used in the State of Michigan for public schools, the school offers classes in Arabic language, Quranic recitation and Islamic Studies. The mission of the school is to provide students with the basic knowledge required to preserve their Islamic heritage, religion and cultural identity.

44. MCA has spent a significant amount of time, staff resources, and funds discussing the impact of September 11th and the Patriot Act on the civil rights of Muslims. It sponsored civil rights forums on January 26, 2002; April 14, 2002; October 13, 2002; and March 12, 2003. Each of these forums addressed the impact of the Patriot Act. The MCA has also sponsored numerous rallies and fundraisers related to the Rabih Haddad case; at these events, the Patriot Act was almost always discussed.

45. Because of the relationship between MCA, its members and leaders, and persons and organizations investigated, questioned, detained, or arrested since September 11th, MCA reasonably believes that the FBI has used or is currently using Section 215 to obtain records or personal belongings about it and its members, students, and constituents.

46. For example, the MCA, its leadership, and its members have been associated with Rabih Haddad. Rabih Haddad is a 41-year-old native of Lebanon who came legally to the United States and lived until recently in Ann Arbor with his wife and four children. He was an active member of MCA and a volunteer teacher at MCA's Michigan Islamic Academy. In 1992, he co-founded the Global Relief Foundation, a humanitarian organization which the federal government has accused of having provided material support for terrorism. In December 2001, Mr. Haddad was arrested on immigration charges. Though never accused of threatening or harming anyone, Mr. Haddad was denied bond and held in solitary confinement for months with almost no access to his family or the outside world. The INS commenced removal proceedings against him based on visa violations, and the government attempted to close the INS hearings to the press and public. The ACLU, the Detroit Free Press, Representative John Conyers and others successfully sued to open the hearings. Mr. Haddad was ultimately imprisoned for approximately nineteen months, and deported to Lebanon in July 2003. He was never charged with any crime.

47. Some MCA members founded the Free Rabih Haddad Committee in December 2001. The Free Rabih Haddad Committee supported the Haddad family during Mr. Haddad's imprisonment, raised money to assist in his defense, organized public demonstrations in support of Mr. Haddad, and organized a letter-writing campaign. The Free Rabih Haddad Committee continues to educate the public about the government's treatment of Mr. Haddad. The MCA itself also held numerous fundraisers and public rallies to protest Mr. Haddad's detention.

48. Almost all meetings of the Free Rabih Haddad Committee were held at the MCA. During his detention, Mr. Haddad placed weekly telephone calls to the MCA in order to speak with MCA leaders and members.

49. The MCA, its leadership, and its members have also been associated with Dr. Sami Al-Arian. In October 2002, Dr. Sami Al-Arian spoke at the MCA mosque on the "Eroding Status of Our Civil Liberties." Dr. Al-Arian is a Kuwaiti-born former professor at the University of South Florida. He was indicted in the Middle District of Florida in February 2003 for allegedly aiding and abetting terrorism in the occupied West Bank. The federal government has introduced evidence in the case that they obtained through wiretaps authorized under another Patriot Act amendment to FISA. Dr. Al-Arian's daughter, Layla Al-Arian, spoke about her father's case at MCA's mosque in March 2003.

50. Other MCA members and leaders have been individually targeted for investigation by the FBI.

51. For example, MCA member Homam Albaroudi was born in Syria and came to the United States in 1987. He received a Masters in Engineering from Missouri State University and a Ph.D. in Engineering from Oregon State University. He is now a United States citizen. He is married to a United States citizen and has three children, all United States citizens. He works as an engineer for a Fortune 100 company.

52. Mr. Albaroudi has been an active member of MCA since 1999. He was a member of the Michigan Islamic Academy's board of directors for 3 years.

53. Mr. Albaroudi has also been a member of CAIR's Michigan chapter for approximately three years.

54. In 1993, Mr. Albaroudi co-founded the Islamic Assembly of North America ("IANA"), a non-profit organization dedicated to educating the public about Islam. While he was associated with the organization, IANA organized conferences, published religious books, and supplied Qurans to incarcerated Muslims. Mr. Albaroudi served as IANA's Executive Director from the organization's founding in 1996 until 1997, when he stepped down from his position and ended his association with IANA because of personal differences with other IANA leaders. The FBI raided IANA's offices in February 2003, seizing computers and taking photographs of books. The computers contained information about Mr. Albaroudi. FBI agents also questioned IANA associates and ex-employees about Mr. Albaroudi, notwithstanding that his association with IANA ended in 1997.

55. Mr. Albaroudi was also a founder of the Free Rabih Haddad Committee. Mr. Albaroudi convened the initial meeting of the Committee on the premises of the MCA.

56. Mr. Albaroudi has twice been contacted by the FBI. On the first occasion, which was approximately four years ago, Mr. Albaroudi was on an employment-related consulting assignment in Indiana when the FBI came looking for him at his home in Michigan. When the FBI discovered that Mr. Albaroudi was not at home, they left their cards with Mr. Albaroudi's wife, asking that Mr. Albaroudi contact them when he returned. Mr. Albaroudi did so. The FBI did not pursue efforts to speak with Mr. Albaroudi after he informed them that he did not feel comfortable speaking with them without an attorney present.

57. The FBI contacted Mr. Albaroudi again in or about March 2003. On this occasion, the FBI agents who contacted him said that they had not singled him out but rather were interviewing many people in the area to find out whether anyone had learned of conspiracies against the United States. Mr. Albaroudi explained to the FBI that he would have contacted them of his own accord if he had learned of conspiracies against the United States. The FBI then asked Mr. Albaroudi about another co-founder of IANA, who had recently been arrested for an overdraft check and then detained on immigration charges. The FBI did not pursue efforts to speak with Mr. Albaroudi after he informed them that he did not feel comfortable speaking with them without an attorney present.

58. Mr. Albaroudi reasonably believes that, because of his religion, his ethnicity, his place of birth, his earlier leadership role in IANA, his leadership role in the Free Rabih Haddad Committee, and his membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain his records and personal belongings.

59. MCA member Kristine Abouzahr was born in Lansing, Michigan in 1958. She is married and has five children, the eldest of whom is 21 and the youngest 9. Mrs. Abouzahr received a B.S. from Oklahoma State University in 1978 and an M.A. from Virginia Polytechnic Institute and State University in 1980. She moved to Michigan in 1986.

60. Mrs. Abouzahr has been a member of the MCA since 1986.

61. Mrs. Abouzahr taught at the Michigan Islamic Academy from 1990-1994, from 1995-1997, from 1999-2001, and during this past academic year. Mrs. Abouzahr's youngest daughter is currently a student at the Michigan Islamic Academy.

62. Mrs. Abouzahr serves on MCA's Outreach Committee, whose mandate is to educate Americans about Islam. As a member of the Outreach Committee, she has visited numerous local schools and community organizations to give presentations about Islam. Mrs. Abouzahr also serves informally as an advisor to Michigan Islamic Academy's new immigrant students and their parents who have questions about adjusting to life in the United States.

63. Mrs. Abouzahr is an active member of the Ann Arbor Area Committee for Peace (AAACP). As a member of that organization, Mrs. Abouzahr attended demonstrations against the Gulf War, against the Patriot Act, against the FBI's "voluntary" interview program, and in favor of a just peace between Israel and Palestine. Mrs. Abouzahr has also spoken publicly at demonstrations sponsored by AAACP and MCA, including at demonstrations in support of Rabih Haddad.

64. Mrs. Abouzahr is also an active member of the Free Rabih Haddad Committee. As one of the Committee's two Media Coordinators, she drafts press releases, speaks to the media, and organizes public demonstrations. She has also spoken publicly in support of Mr. Haddad. For example, in February 2002, after she had traveled to Washington, D.C., with Mr. Haddad's wife, she spoke at an informational forum organized and co-sponsored by the AAACP and the Free Rabih Haddad Committee to inform the local community about Haddad's case.

65. The Free Rabih Haddad Committee's post office box is registered in Mrs. Abouzahr's name.

66. Mrs. Abouzahr reasonably believes that, because of her religion, her leadership role in the Free Rabih Haddad Committee, her membership in AAACP, and

her membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain her records and personal belongings.

67. MCA member Nazih Hassan was born in Lebanon in 1969. He emigrated to Canada in 1988 and became a Canadian citizen in 1993. Mr. Hassan received his B.Esc. from the University of Western Ontario in 1994.

68. Mr. Hassan came to the United States in 1994 to study at Eastern Michigan University. He received his M.S. in Computer Information Systems from that institution in 1997.

69. Mr. Hassan became a legal permanent resident in 2001. He is married and has three children, two of whom are United States citizens. Mr. Hassan now works as a technology consultant and resides in Ypsilanti, Michigan.

70. Mr. Hassan has been a member of the MCA since 1994. Since January 2002, he has served as MCA's President. At various times since 1995, he also served as Editor of MCA's newsletter, as MCA's Secretary, and as MCA's Vice President.

71. Mr. Hassan was a founder of the Free Rabih Haddad Committee. As one of the Committee's two Media Coordinators, he drafts press releases, speaks to the media, and organizes public demonstrations.

72. Mr. Hassan reasonably believes that, because of his religion, his ethnicity, his place of birth, his leadership role in the Free Rabih Haddad Committee, and his membership and leadership role in MCA, the FBI has used or is currently using Section 215 to obtain his records and personal belongings.

73. MCA also reasonably believes that it could be served with a Section 215 order. It then would have no ability to challenge the order before compromising the

privacy and free speech rights of its members. MCA maintains various records pertaining to its members, including records of members' names, telephone numbers, e-mail, home and business addresses, and citizenship status and national origin. MCA keeps records relating to members' marriages and divorces, and relating to members' family problems that MCA's Imam and Social Committee help resolve. MCA also keeps records documenting the use of zakat (members' charitable donations). The Michigan Islamic Academy also maintains a variety of educational and counseling records about its students. Finally, MCA has a variety of religious documents associated with the mosque and the Michigan Islamic Academy.

74. MCA has a policy of strictly maintaining the privacy of its records and routinely assures its members that any information they provide to MCA will be kept confidential. MCA's members rely on MCA's assurances that their records will be kept confidential.

75. Section 215 compromises MCA's ability to maintain the confidentiality of records pertaining to its members and students, and to protect individual members and students from harassment, threats, and violence. MCA has been the target of harassment since September 11th. For example, on some occasions after MCA President Nazih Hassan was quoted in newspaper articles, the MCA received several hate letters. After Mr. Hassan wrote a letter to the Ann Arbor News at the end of March 2003, an unknown individual or group placed hate fliers on cars outside the mosque. Were the confidentiality of MCA's records to be compromised and MCA's membership list to become public knowledge, MCA's individual members would be subjected to verbal harassment, threats, and even violence.

76. MCA's ability to keep its records confidential also allows MCA to protect its members and students from the possibility that the government will target them for their exercise of First Amendment rights, including their rights to free speech, free association, and free exercise of religion.

77. Because of the likelihood that the FBI is using provisions of the Patriot Act to target MCA, its leadership, and its members, some MCA members are afraid to attend mosque, to practice their religion, or to express their opinions about religious and political issues. Several people have told MCA leaders that they do not attend mosque for fear that the FBI is surveilling MCA and intends to investigate those who are associated with the organization.

American-Arab Anti-Discrimination Committee

78. ADC is a non-profit civil rights organization committed to defending the rights and promoting the rich cultural heritage of people of Arab descent. ADC has members and volunteer-based chapters in many states. It is headquartered in Washington, D.C., and has staffed offices in New York City, Detroit, San Diego, and San Francisco.

79. Since the passage of the Patriot Act, ADC has spent a significant amount of time, staff resources, and funds in advocating against the civil rights encroachments authorized by the Act. ADC has co-sponsored congressional briefings in Washington, D.C., and held town hall meetings throughout the country to educate the public about the Act. Most recently, ADC was a major co-sponsor of a national congressional briefing held on Capitol Hill on June 4, 2003. The briefing, which was attended by several prominent senators and representatives, featured testimony from immigrants who had

suffered civil rights violations after September 11th. On June 2, 2003, ADC co-sponsored another congressional staff briefing focusing on the Act and other post-September 11 Department of Justice initiatives. ADC staff members have spoken about the Patriot Act at over 150 conferences, seminars, and university events around the nation. Additionally, ADC's National Conventions for 2002 and 2003 included several panels discussing the Patriot Act and other government programs and policies implemented after the Patriot Act became law. ADC spokespeople, including Communications Director Hussein Ibish, are among the leading advocates in national media against the Patriot Act. Moreover, the ADC Legal Department provides routine assistance to anyone contacting ADC for help concerning law enforcement or other activities related to the Patriot Act. Finally, ADC's Legal Department is an active participant in coalition-based policy advocacy to amend or repeal parts of the Act.

80. ADC monitors the due process and equal protection rights of all Arab-Americans, including those who were detained on by the INS after September 11th and those who have been caught up in terrorism investigations.

81. For example, ADC and its members publicly condemned the use of secret evidence in the detention of Dr. Mazen Al-Najjar, formerly a University of South Florida professor. Though incarcerated for over three years, Dr. Al-Najjar was never charged with any criminal offense. He was ultimately deported for visa violations.

82. ADC and its members have also made public statements of concern about due process issues in the case of Rabih Haddad, a community leader in Ann Arbor, Michigan who was detained by the INS in December 2001, imprisoned for approximately

nineteen months, and ultimately deported in July 2003 without having been charged with any crime.

83. Because of the relationship between ADC, its members, and persons questioned, detained, or deported since September 11th, ADC reasonably believes that the FBI has used or is currently using Section 215 to obtain records and personal belongings about it and its members.

84. ADC also reasonably believes that it could be served with a Section 215 order. ADC would then would have no ability to challenge the order before compromising the privacy rights of its members. ADC maintains a variety of records about members, including their names and names of family members, home and business mailing addresses, phone numbers, email addresses, credit card information, and checking account information. ADC has a policy of maintaining the confidentiality of its members and their private information. ADC does not disclose membership numbers or any other information about members.

85. Section 215 compromises ADC's ability to maintain the confidentiality of records pertaining to its members, and to protect members from harassment, threats, and violence. ADC has documented a substantial increase in hate crimes, discrimination, and harassment against Arab-Americans since the September 11th attacks. Many of these incidents are described in the ADC publication, "Report on Hate Crimes and Discrimination Against Arab Americans; The Post-September 11 Backlash." Over 700 violent incidents occurred in the first nine weeks following the attack, including several murders. In the first year after the attacks, ADC documented over 80 cases in which airlines had discriminated against passengers who were perceived to be Arab. There

were also over 800 cases of employment discrimination against Arab-Americans, an approximately four-fold increase over previous annual rates, and numerous instances of denial of service, discriminatory service and housing discrimination. These numbers remain significantly above pre-September 11th levels today. Were the confidentiality of ADC's records to be compromised or ADC's full membership list to become public knowledge, ADC's members could risk harassment, threats, and even violence.

Arab Community Center for Economic and Social Services

86. ACCESS is a human services organization committed to the development of the Arab-American community in the United States. Its staff and volunteers serve low-income families, help newly arrived immigrants adapt to life in the United States, and educate Americans about Arab culture. ACCESS provides a wide range of social, mental health, educational, artistic, employment, legal and medical services. ACCESS has more than 2500 members and approximately 150 full-time staff.

87. ACCESS provides over seventy different programs to more than a hundred thousand people of all ethnic and religious backgrounds. In the last fiscal year, ACCESS provided more than 57,290 services in the area of social and legal services, more than 12,600 counseling and psychiatric services, more than 60,300 in health and health education services, and more than 55,600 employment and vocational services. ACCESS also provided more than 256,590 hours of educational and recreational services to youths and their parents, and sponsored cultural events and activities attended by many thousands of people.

88. For example, ACCESS runs a Community Health and Resources Center that offers a wide range of medical, public health, mental health and family counseling

services and programs. Its division of Psychosocial Rehabilitation for Survivors of Torture and Refugee Family Strengthening provides mental health services to torture victims and refugees. ACCESS also provides specialized services to victims of domestic violence, administers a breast and cervical cancer control program, and provides HIV/AIDS and STD education, counseling and testing. The Center's research division has twice sponsored a National Conference on Health Issues in the Arab Community.

89. ACCESS's Department of Social Services offers emergency food assistance, immigration services, and homelessness prevention programs. Its Department of Employment and Training offers a variety of job training programs, language instruction, and family acculturation services to help immigrants integrate into their new society. The Youth and Education Department provides after school homework assistance to students, special programs for at-risk youth, and recreation programs and teen dialogue opportunities for young people.

90. Because of the relationship between ACCESS, its members and clients, and persons questioned, detained, or deported since September 11th, ACCESS reasonably believes that the FBI has used or is currently using Section 215 to obtain records or other personal belongings about it and its members and clients.

91. Some of ACCESS's members and clients have been individually targeted for investigation by the FBI.

92. For example, ACCESS member Ahmad Ali Ghosn was born in Lebanon in 1965. He has been a legal permanent resident of the United States since 1993. Mr. Ghosn's application for naturalization has been pending for over seven years. Mr. Ghosn first submitted his application in June 1996. The INS later informed Mr. Ghosn that it

had lost the application and advised him to submit two duplicate applications. Mr. Ghosn did so. He received an acknowledgement notice from the INS in January 1998 – over five years ago. Since January 1998, the INS has required Mr. Ghosn to be fingerprinted on multiple occasions but it has never sought to schedule a naturalization interview.

93. The INS most recently required Mr. Ghosn to be fingerprinted in February 2002. When Mr. Ghosn appeared as he had been asked to, he was greeted not only by an INS criminal investigator but also by two FBI agents, who questioned him for over two hours about his associations with various individuals and charitable organizations in Lebanon. The FBI agents informed Mr. Ghosn that he could be naturalized if he cooperated with them, but that if he did not, his children would be seized by the government and placed in foster care. Mr. Ghosn answered the FBI's questions to the best of his ability but refused their request that he become an FBI or INS spy. He was not advised of his right to counsel.

94. Because of the FBI's actions, Mr. Ghosn reasonably believes that the FBI has used or is currently using Section 215 to obtain his records or other personal belongings.

95. ACCESS also reasonably believes that it could be served with a Section 215 order. It would then have no ability to challenge the order before compromising the privacy rights of its members and clients. ACCESS maintains a wide range of highly personal, sensitive records relating to the services it offers to clients. For example, the Community Health and Research Center maintains medical records for torture victims and refugees, and for breast cancer, mental health, and HIV/AIDS patients. It also

maintains files on domestic violence victims and family counseling clients. ACCESS routinely assures its clients that the information they provide will be kept confidential.

Bridge Refugee & Sponsorship Services

96. Bridge is an ecumenical, non-profit organization that helps refugees and asylum-seekers become and stay self-sufficient.

97. Bridge is affiliated with Church World Service ("CWS"), which is the relief, development, and refugee assistance ministry of 36 Protestant, Orthodox, and Anglican denominations in the United States, and with Episcopal Migration Ministries ("EMM"), which is the arm of the Episcopal Church that advocates for the protection of the refugees.

98. Bridge employs eight staff members and has offices in Knoxville, Chattanooga, and Bristol, Tennessee.

99. Bridge generally obtains clients in either of two ways. In some cases, a person residing in the United States asks Bridge to assist a relative whom the United States has granted refugee status but who has not yet arrived in the United States. In these cases (called "family reunification" cases), Bridge begins working with the refugee's family while the refugee is still outside the United States. In other cases, Bridge is assigned refugees' files by affiliate organizations such as CWS and EMM. These cases (called "free" cases) usually involve refugees who do not have family in the United States.

100. Historically, Bridge has served approximately 200 new refugees and asylum seekers in a year. Bridge's current caseload, which includes refugees who arrived in the United States over the last five years, includes approximately 500 files.

101. Bridge ordinarily serves its clients through individual sponsors, whom Bridge recruits from local churches, mosques, and synagogues.

102. Sponsors sign confidentiality agreements. Bridge staff explain and review the confidentiality agreement in sponsor training sessions.

103. Bridge provides its clients with a broad spectrum of resettlement services. For example, Bridge staff and sponsors ensure that new refugees have accommodations, furniture, clothing, and food; accompany new refugees to the Department of Health for medical examinations and immunizations; provide English language tutors to refugees who require them; ensure that refugee children enroll in school; provide cultural counseling to educate new refugees about American customs; assist new refugees in finding employment as quickly as possible; assist new refugees in complying with immigration requirements; assist refugees in applying for permanent residence and citizenship; direct refugees to social services provided by other organizations or by the federal and state governments; and counsel refugees about personal problems, including substance abuse, sexual abuse, discrimination at work or school, domestic violence, family planning, and divorce.

104. Bridge maintains various records pertaining to its clients, including records of clients' names, telephone numbers, and residential addresses. Bridge also keeps records of its clients' dates of arrival in the United States.

105. In many cases, Bridge's files also include case notes taken by Bridge staff. Case notes may document medical conditions from which the client has suffered in the past or that the client suffers currently. Case notes may also document the nature of the persecution that the client faced in her home country.

106. In some cases, clients consult Bridge staff about personal problems, including substance abuse, sexual abuse, discrimination at work or school, domestic violence, family planning, and divorce. In one case, for example, Bridge counseled a client about a venereal disease that she had acquired as a result of rape by a soldier. In another case, Bridge counseled an elderly client who was being mistreated by his daughters. Bridge's case notes include documentation of conversations relating to these and similarly intimate, personal problems.

107. In many cases, Bridge's refugee clients can obtain the assistance they need only from Bridge. There is no other resettlement services organization in East Tennessee whose staff have the relevant language and professional skills. When Bridge's clients decide that they cannot afford to entrust their personal information to Bridge, those clients generally do not obtain the help that they need from anywhere. They simply deal with their problems – including serious medical and personal problems – on their own.

108. Bridge is concerned that Section 215 compromises its ability to maintain the confidentiality of its clients' records. Bridge regularly assures its clients that the information they provide will be kept confidential, and explains that, under state law, the confidentiality of the information that clients provide is protected by a social worker privilege. Bridge provides its clients with a confidentiality agreement that assures clients that Bridge will disclose their records only "to facilitate the continuation of proper medical treatment and social services."

109. Bridge reasonably believes that it could be served with a Section 215 order. Bridge would then would have no ability to challenge the order before compromising the privacy rights of its members.

110. The FBI has approached Bridge for information about its clients on at least two occasions. In early November 2002, the FBI approached Bridge to ask it to disclose all records relating to its Iraqi-born clients. Bridge declined to disclose the records because the records included sensitive, personal information, including medical information.

111. On November 12, 2002, Bridge was served with a Subpoena To Testify Before Grand Jury, ordering the production of "Any and all records of Bridge . . . relating to any and all Iraqi-born people who have been assisted by Bridge Refugee and Sponsorship Services, Inc., including records that provide the name, address, telephone number, employer, and personal circumstances of such persons." Bridge moved to quash the subpoena but withdrew its motion when the FBI agreed not to seek more information than Bridge's clients would already have provided to the INS. The FBI made clear, however, that it might eventually demand more information. The FBI did not indicate what form such a demand might take.

112. Bridge client Muwafa Albaraqi was born in 1968 in Najaf, Iraq, where he lived until 1991. In 1991, at the encouragement of the United States, Mr. Albaraqi participated in an uprising against the government of Saddam Hussein. Although the uprising was successful in Najaf, American support did not materialize and ultimately the city fell again to the Iraqi Republican Guard. Those who had participated in the uprising were labeled traitors and were tortured, imprisoned, or killed. Mr. Albaraqi fled to Saudi Arabia.

113. Mr. Albaraqi lived in a United Nations-administered refugee camp in Saudi Arabia from March 1991 to September 1994. He applied for political asylum in the United States while living at the camp.

114. Mr. Albaraqi came to the United States in September 1994. His file, which was initially assigned to another refugee organization, was transferred to Bridge when Mr. Albaraqi decided that he would reside in Tennessee, where he had friends.

115. Bridge assisted Mr. Albaraqi in adjusting to life in Tennessee. For example, Bridge showed Mr. Albaraqi around Knoxville, pointing out where he could buy groceries and clothing, and showed him how to use the bus system. Bridge helped Mr. Albaraqi find a place to live, paid his first month's rent and utilities, and bought him groceries for his first week in the country. Bridge also helped Mr. Albaraqi apply for federal assistance, including food stamps and social security. Bridge accompanied Mr. Albaraqi to the Department of Health, where Mr. Albaraqi was given a medical examination and immunizations. Bridge also helped Mr. Albaraqi with his application for permanent residence and, eventually, his application for citizenship.

116. Mr. Albaraqi became a United States citizen in 1999. Mr. Albaraqi now works as a check-out clerk at a grocery store in Knoxville, Tennessee. He is also a part-time student in electrical engineering at the University of Tennessee.

117. The FBI came to Mr. Albaraqi's workplace in January 2003, stating that they wanted to talk to him. Mr. Albaraqi was not told that the interview was optional or voluntary or that he had a right to contact an attorney and have an attorney present at the interview.

118. During the interview, the FBI asked, among other questions, whether anyone associated with the Iraqi government had asked him to engage in terrorism against American targets; what he would do if an Iraqi agent asked him to engage in terrorism; and whether he might act differently if the Iraqi agent cut off his brother's finger and sent it to him in the mail.

119. Mr. Albaraqi would not have sought Bridge's assistance for sensitive, personal matters had he thought that the FBI could easily access Bridge's records under Section 215. Based on his own experience as a refugee, he believes that other refugees will be less likely to seek help from Bridge because the FBI can obtain their sensitive, personal records even when they have done nothing wrong.

Council on American-Islamic Relations

120. CAIR is a non-profit, grassroots organization dedicated to enhancing the public's understanding of Islam and Muslims. CAIR is the largest Islamic civil liberties organization in the United States. CAIR's national office in Washington, D.C., has a permanent staff of about 25 people. Approximately the same number of people are employed by CAIR's state and local chapters.

121. Since the passage of the Patriot Act, CAIR has spent a significant amount of time, staff resources, and funds in advocating against the civil rights encroachments authorized by the Act. CAIR hosts an annual conference each March. At both the 2002 and 2003 conferences, multiple speakers explained the Patriot Act and discussed its import for Muslims in the United States. CAIR hosts an annual dinner each October. At both the 2001 and 2002 dinners, speakers explained the Patriot Act and discussed its import for Muslims in the United States. CAIR regularly distributes e-mail "Action

Alerts" to members and others who have subscribed to CAIR's Action Alert list. Since the Patriot Act became law, CAIR has distributed numerous Action Alerts related to the Patriot Act. CAIR has also issued numerous news releases related to the Patriot Act.

122. CAIR monitors the due process and equal protection rights of all Muslims living in the United States, including those detained on immigration charges after September 11th and those caught up in terrorism investigations. In 2002, CAIR issued a 54-page "Civil Rights Report" that, among other things, examined the impact that "anti-terrorism" policies, including the Patriot Act, had had on the civil liberties of American Muslims. CAIR issued a similar Civil Rights Report in 2001 and issued a new Civil Rights Report in July 2003.

123. Because of the relationship between CAIR, its members, and persons questioned, detained, or deported since September 11th, CAIR reasonably believes that the FBI is currently using Section 215 to obtain records and personal belongings of CAIR and its members.

124. For example, CAIR member Magda Bayoumi was born in Cairo, Egypt, in 1956. She came to the United States in 1977 and became a United States citizen in 1988. Mrs. Bayoumi has been a member of CAIR for approximately four years.

125. Mrs. Bayoumi is married and has three children, of whom the youngest is 10 and the eldest 17. Mrs. Bayoumi's husband was also born in Cairo, Egypt. He became a United States citizen in 1991. All of Mrs. Bayoumi's children are United States citizens. Mrs. Bayoumi and her family live in Syracuse, New York.

126. Mrs. Bayoumi works as a volunteer for several community organizations. She currently chairs the board of the Parents Advisory Group for the Special-Education

Director of the Syracuse School District. She serves as a board member of the Central New York Parent's Coalition for Children With Special Needs. She co-founded and serves on the board of the of Autism Support Group. She founded and serves on the board of the Ed Smith School's Support Group for Children With Special Needs.

127. Mrs. Bayoumi and her husband co-founded and serve on the board of the Central New York Chapter of the American Muslim Council, an organization that was established in 1990 to increase the effective participation of American Muslims in the political process.

128. Two FBI agents came to Mrs. Bayoumi's home on February 26, 2003. They first informed Mrs. Bayoumi that they wanted to question her husband. When Ms. Bayoumi told the agents that her husband was not at home, however, they began to question her instead.

129. The FBI's questioning focused on a donation that Mrs. Bayoumi and her husband had made to a charity called Help the Needy. Mrs. Bayoumi and her husband had donated several hundred dollars to the organization the previous year.

130. The agents asked Mrs. Bayoumi how much money she and her husband had contributed to the charity, whether she had attended a dinner that Help the Needy had recently hosted, whether she knew what the donation was being used for, and whether she would be upset if the money had been used to build a mosque. Mrs. Bayoumi told the FBI that she and her husband had donated a few hundred dollars to the charity in each of the previous few years, had attended the recent dinner, and had assumed that the donation would be used to provide food and medicine for needy people in Iraq.

131. The FBI did not inform Mrs. Bayoumi how they had learned that she and her husband had made a donation to Help the Needy.

132. On the same day that the FBI questioned Mrs. Bayoumi, the Department of Justice announced that a federal grand jury in Syracuse, New York, had returned an indictment charging Help the Needy and four individuals associated with it of transferring funds to persons in Iraq without having obtained the proper license. While Help the Needy was not accused of having providing anything other than humanitarian aid to people living in Iraq, the Justice Department's press release accused Help the Needy of attempting to undermine the President's efforts "to end Saddam Hussein's tyranny and support for terror."

133. Mrs. Bayoumi reasonably believes that because of her religion, her ethnicity, and her earlier support for Help the Needy, the FBI has used and is currently using Section 215 to obtain her records and other personal belongings.

134. CAIR also reasonably believes that it could be served with a Section 215 order. CAIR would then would have no ability to challenge the order before compromising the privacy rights of its members. CAIR maintains a variety of records about members, including their names, home and business mailing addresses, phone numbers, email addresses, credit card information, and checking account information. CAIR has a policy of maintaining the confidentiality of its members and their private information. CAIR does not disclose membership numbers or any other information about individual members.

135. Section 215 compromises CAIR's ability to maintain the confidentiality of records pertaining to its members, and to protect members from harassment, threats, and

violence. CAIR has documented a substantial increase in hate crimes, discrimination, and harassment against Muslim and Arab-Americans since the September 11th attacks. Many of these incidents are described in CAIR's 2001, 2002, and 2003 Civil Rights Reports. Were the confidentiality of CAIR's records to be compromised and CAIR's membership list to become public knowledge, CAIR members could risk harassment, threats, and even violence.

Islamic Center of Portland, Masjed As-Saber

136. The Islamic Center of Portland, Masjed As-Saber ("ICPMA"), is a non-profit organization that owns and administers a mosque known as Masjed As-Saber and an Islamic school known as the Islamic School of Portland. Approximately 450 people attend services at the mosque each Friday; as many as 3500 attend services on religious holidays. ICPMA employs approximately 16 people. Approximately 60 students are enrolled at the school.

137. Because of the relationship between ICPMA, its community members and leaders, and persons and organizations investigated, questioned, detained, or arrested since September 11th, ICPMA reasonably believes that the FBI has used or is currently using Section 215 to obtain records and personal belongings pertaining to it and its community members and students.

138. Some ICPMA community members have been individually targeted for investigation by the FBI.

139. In October, 2002, a federal grand jury in the District of Oregon indicted six individuals and charged them with various counts of conspiracy to wage war against the United States and to provide material support to Al Qaeda; a seventh individual was

indicted on similar charges in April 2003. A trial is currently scheduled for January 2004 in this case, which is known as the "Portland 7" case. Some of the defendants, Jeffrey Leon Battle, Patrice Lumumba Ford, and Habis Abdulla al Saoub, attended the ICPMA. In an affidavit submitted in support of the indictment of the defendants, Police Officer Thomas W. McCartney stated that a wired informant recorded conversations inside the Islamic Center of Portland, Masjed As-Saber, on June 6, 2002. The electronic surveillance was authorized under another Patriot Act amendment to FISA. The affidavit also states that the government obtained a number of records relating to the investigation. The affidavit does not state the legal authority utilized in obtaining these records. The government has stated publicly that the investigation into the alleged conspiracies is ongoing.

140. The FBI has also sought records from ICPMA. In March 2003, the ICPMA was served with a subpoena seeking financial records related to the defendants and their spouses in the Portland 7 case. ICPMA retained lawyers who moved to quash the subpoena because of the impact on the privacy rights of ICPMA's constituents, but was ultimately required to disclose the records. Some of ICPMA's constituents are now afraid to donate to ICPMA because they fear their donations will provoke FBI investigation and harassment. The FBI has also served subpoenas to over 25 people in the Portland area, some of whom attend ICPMA and other local mosques. The FBI has interviewed some ICPMA community members and has asked questions about other worshipers and their political and religious views.

141. In addition, some of ICPMA's leaders appear to be under investigation by the FBI but have not been charged with any crime.

142. For example, ICPMA president Alaa Abunijem was born in Saudi Arabia and came to the United States in 1989. He became a U.S. citizen in 1996. Mr. Abunijem is married to a U.S. citizen and has four children. He holds a B.S. degree in Electrical Engineering and an M.S. in Engineering and Technology Management. He currently works as an engineer for a Fortune 100 company, and has lived in Portland, Oregon, since 1999.

143. On December 17, 2002, Mr. Abunijem was stopped at the Seattle airport by U.S. Customs and questioned by both U.S. customs and FBI officials regarding the purpose of his trip to Saudi Arabia. The officials searched his documents, business cards, and credit cards for thirty minutes before returning them to him. On his return from Saudi Arabia on January 9, 2003, his luggage and documents were searched for over an hour and a half, and he was questioned by officials about his trip.

144. On February 26, 2003, an FBI agent called Mr. Abunijem at his work place and questioned him about a donation he had made to a charity called Help the Needy. Mr. Abunijem had made donations of several hundred dollars to the organization over the past few years. The FBI did not inform Mr. Abunijem how they had learned that he made a donation to Help the Needy. Mr. Abunijem told the FBI agent that he did not feel comfortable talking to the FBI without a lawyer.

145. On the same day that the FBI questioned Mr. Abunijem, the Department of Justice announced that a federal grand jury in Syracuse, New York, had returned an indictment charging Help the Needy and four individuals associated with it of transferring funds to persons in Iraq without having obtained the proper license. While Help the Needy was not accused of having providing anything other than humanitarian

aid to people living in Iraq, the Justice Department's press release accused Help the Needy of attempting to undermine the President's efforts "to end Saddam Hussein's tyranny and support for terror."

146. Since 1999, Mr. Abunijem has served as a board member of the Islamic Assembly of North America ("IANA"), a non-profit organization dedicated to educating the public about Islam. IANA organizes conferences, publishes religious books, and supplies Qurans to incarcerated Muslims. The FBI raided IANA's offices in Michigan in or about February 2003, seizing computers and taking photographs of books. The computers contained information about Mr. Abunijem. The government has not charged IANA with any crime, but has arrested one of the organization's former presidents, Bassem K. Khafagi, on federal bank fraud charges. Assistant U.S. Attorney Terry Derden of Boise, Idaho has stated publicly that "the investigation could expand to other directors and Islamic Assembly employees."

147. Mr. Abunijem has not been charged with any crime and strongly maintains his innocence.

148. Mr. Abunijem reasonably believes that because of his religion, his ethnicity, his place of birth, his leadership role in ICPMA and IANA, and his donations to Help the Needy, the FBI is currently using Section 215 to obtain his records and personal belongings.

149. ICPMA reasonably believes that it could be served with a Section 215 order. It would then have no ability to challenge the order before compromising the privacy rights of its members. ICPMA maintains a variety of records about community members, including their names and the names of family members, home and business

mailing addresses, phone numbers, email addresses, credit card information, and checking account information. ICPMA also retains records of services it provides to community members, including Islamic marriage contracts, and records of divorce proceedings and financial assistance given to needy families. The Islamic School of Portland retains health, financial and educational records pertaining to all of its students and staff. ICPMA has a policy of maintaining the confidentiality of all records pertaining to its community members, staff and students.

150. Section 215 compromises ICPMA's ability to maintain the confidentiality of its records, and to protect community members and students from harassment, threats, and violence. Since the September 11th attacks, ICPMA community members and other Arab-Americans have repeatedly been the target of harassment. Were the confidentiality of ICPMA's records to be compromised and ICPMA's community list or other records to become public knowledge, ICPMA's community members and students could risk verbal harassment, threats, and even violence.

151. ICPMA's ability to keep its records confidential also allows ICPMA to protect its community members from the possibility that the government will target them for their association with ICPMA, including their rights to free speech, free association, and free exercise of religion.

152. Because ICPMA community members believe that the FBI is currently using provisions of the Patriot Act to target ICPMA, and because the FBI has recorded conversations and services inside the mosque and sought records from ICPMA, many ICPMA community members are afraid to attend mosque, practice their religion, or express their opinions about religious and political issues.

CAUSES OF ACTION

153. Section 215 violates the Fourth Amendment by authorizing the FBI to execute searches without criminal or foreign intelligence probable cause.

154. Section 215 violates the Fourth Amendment by authorizing the FBI to execute searches without providing targeted individuals with notice or an opportunity to be heard.

155. Section 215 violates the Fifth Amendment by authorizing the FBI to deprive individuals of property without due process.

156. Section 215 violates the First Amendment by categorically and permanently prohibiting any person from disclosing to any other person that the FBI has sought records or personal belongings.

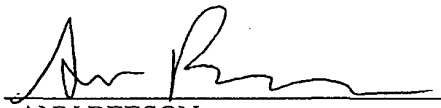
157. Section 215 violates the First Amendment by authorizing the FBI to investigate individuals based on their exercise of First Amendment rights, including the rights of free expression, free association, and free exercise of religion.

PRAYER FOR RELIEF

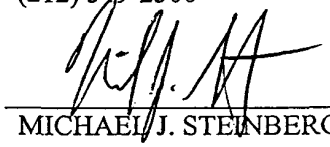
WHEREFORE Plaintiff respectfully requests that the Court:

1. Declare that Section 215 is unconstitutional under the First, Fourth, and Fifth Amendments.
2. Permanently enjoin Defendants from using Section 215.
3. Award Plaintiff fees and costs pursuant to 28 U.S.C. § 2412.
4. Grant such other and further relief as the Court deems just and proper.

Respectfully submitted,



ANN BEESON
JAMEEL JAFFER
National Legal Department
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004-2400
(212) 549-2500



MICHAEL J. STEINBERG
NOEL SALEH
KARY L. MOSS
American Civil Liberties Union Fund
of Michigan
60 West Hancock
Detroit, MI 48201-1343
(313) 578-6800

Dated: July 30, 2003

Written by: Patrick Rowan, OGC
Date/Time: July 18, 2003

Patriot Act: Section 215 - Library/Bookstore Records

Issue: Does Section 215 of the Patriot Act represent a threat to the privacy of those who patronize libraries and bookstores?

Response:

- Section 215 amended the business records authority found in the Foreign Intelligence Surveillance Act (FISA). Under the former language, the FISA Court could issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power.

- The Patriot Act changed the standard to **simple relevance** and authorizes compelled production in relation to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution. The Patriot Act also broadens the categories of items that can be obtained; the authority can now be used for "the production of any tangible thing."

- Section 215 is not a radical expansion of federal investigative authority. Federal grand juries have long had power to issue subpoenas to all types of organizations, including libaries and bookstores, without a probable cause requirement. Several high-profile investigations (Unabomber, NRO spy Brian Regan) involved subpoenas to and/or surveillance in public libraries.

- When we are conducting a covert investigation of a suspected spy or terrorist, it is vitally important that he or she not learn of our request for records. The non-disclosure provision in 215 is also not a radical innovation; similar provisions exist preventing financial institutions (12 USC § 3414) and communications service providers (18 USC § 2709) from disclosing that the FBI obtained information pertaining to customer records.

- The FBI conducted an informal survey of field offices that revealed fewer than 50 contacts with libraries after 9/11. All of those contacts were based on specific leads or subjects. The vast majority of the contacts were based on voluntary reports by library personnel of suspicious behavior by patrons.

- It is important to note that the FBI does not open investigations on how persons exercise their First Amendment rights or on the lawful exercise of any other rights secured by the Constitution or federal statute. FBI counterterrorism investigations are opened, pursuant to the Attorney General Guidelines, based on information indicating terrorist activity.

Certification must state:

(1) Certifying official deems information sought to be foreign intelligence information

(2) That a significant purpose of surveillance is to obtain foreign intelligence information

Foreign intelligence information means

1. information that relates to, and if concerning a US person is necessary to, the ability of the US to protect against —

   A. actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
   B. sabotage or international terrorism by a foreign power or an agent of a foreign power; or
   C. clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power;

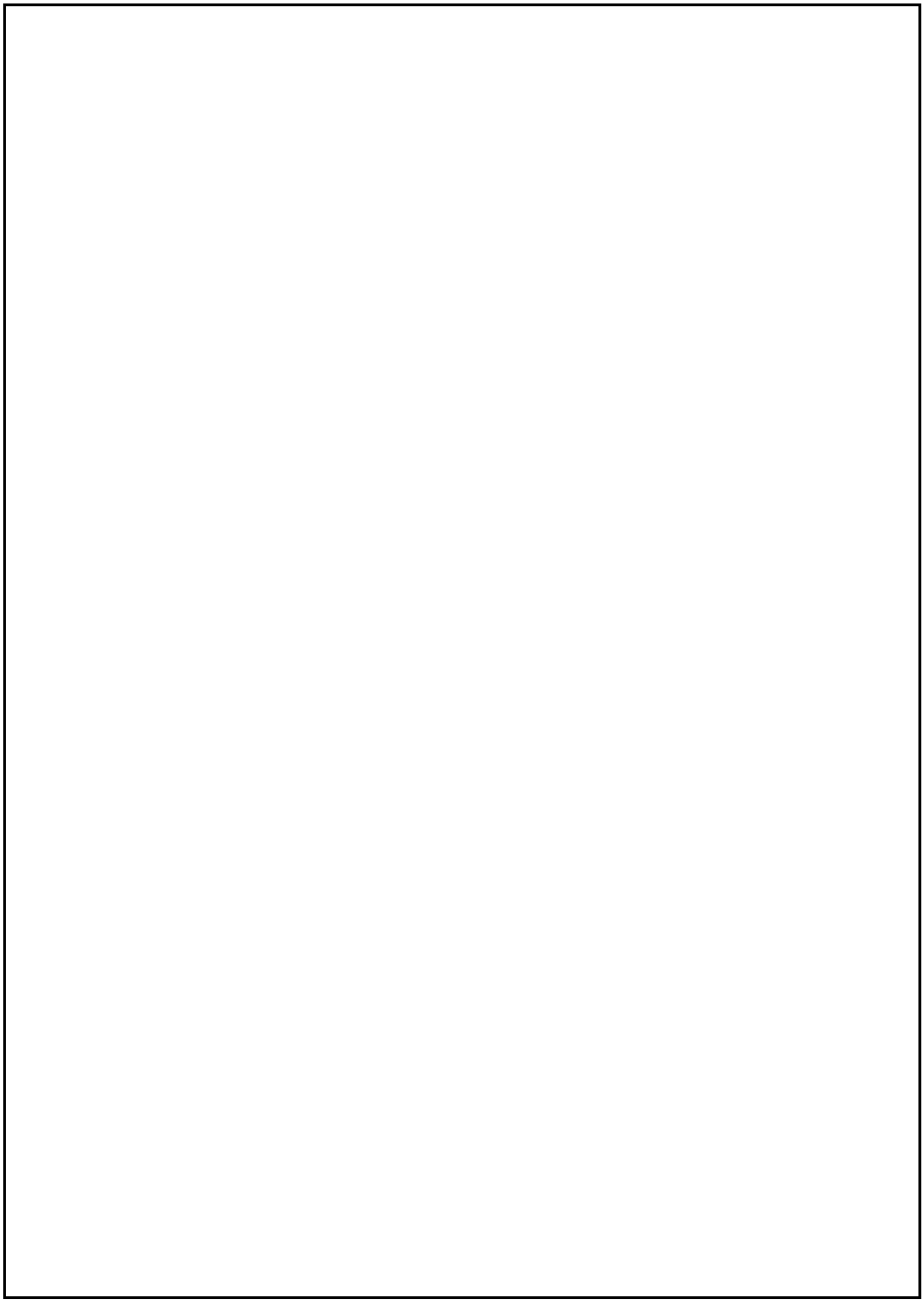
or

2. information with respect to a foreign power or foreign territory that relates to, and if concerning a US person is necessary to —

   A. the national defense or the security of the U.S. or

   B. the conduct of the foreign affairs of the U.S.

b5



b5

b5

Order Code RL30465

CRS Report for Congress

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework

Updated April 29, 2002

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework

Summary

The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, provides a statutory framework for electronic surveillance in the context of foreign intelligence gathering. In so doing, the Congress sought to strike a delicate balance between national security interests and personal privacy rights. Subsequent legislation expanded federal laws dealing with foreign intelligence gathering to address physical searches, pen registers and trap and trace devices, and access to certain business records. P.L. 107-56 made significant changes to some of these provisions. This report will examine the detailed statutory structure provided by the Foreign Intelligence Surveillance Act, as amended (FISA), and related provisions of E.O. 12333. It is current through the changes to FISA in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56, which was signed into law by President George W. Bush on October 26, 2001, and the amendments included in the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, which was signed into law by the President on December 28, 2001.

Contents

The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework

Introduction

On October 26, 2001, President George W. Bush signed P.L. 107-56, the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act or the USA PATRIOT Act. Among its provisions are a number which impacted or amended the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* (FISA). For example, the new law expanded the number of United States district court judges on the Foreign Intelligence Surveillance Court and provided for roving or multipoint electronic surveillance authority under FISA It also amended FISA provisions with respect to pen registers and trap and trace devices and access to business records. In addition, FISA, as amended, substantially expanded the reach of the business records provisions. The amended language changed the certification demanded of a federal officer applying for a FISA order for electronic surveillance from requiring a certification that *the* purpose of the surveillance is to obtain foreign intelligence information to requiring certification that *a significant purpose* of the surveillance is to obtain foreign intelligence information. FISA, as amended, also affords persons aggrieved by inappropriate use or disclosure of information gathered in or derived from a FISA surveillance, physical search or use of a pen register or trap and trace device a private right of action. Of the amendments made by the USA PATRIOT Act, all but the section which increased the number of judges on the Foreign Intelligence Surveillance Court will sunset on December 31, 2005.

This report will provide background on the Foreign Intelligence Surveillance Act, and discuss its statutory framework, as modified by P.L. 107-56. Where applicable, this report will also note the amendments to FISA reflected in P.L. 107-108 (H.R. 2883), the Intelligence Authorization Act for Fiscal Year 2002, which was signed into law by the President on December 28, 2001.

Background

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests.[1] The stage was set for legislation to address these

---

[1]The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no

(continued...)

competing concerns in part by Supreme Court decisions on related issues. In *Katz v. United States*, 389 U.S. 347 (1967), the Court held that the protections of the Fourth Amendment extended to circumstances involving electronic surveillance of oral communications without physical intrusion.[2] The *Katz* Court stated, however, that its holding did not extend to cases involving national security.[3] In *United States v. United States District Court*, 407 U.S. 297 (1972) (the *Keith* case), the Court regarded *Katz* as "implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[4] Mr. Justice Powell, writing for the *Keith* Court, framed the matter before the Court as follows:

> The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.[5]

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.[6] Justice Powell emphasized that the case before it "require[d] no judgment on the scope of the President's surveillance power with respect to the activities of foreign

---

[1](...continued)

> Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[2]*Katz v. United States*, 389 U.S. 347, 353 (1967).

[3]*Id.*, at 359, n. 23.

[4]*United States v. United States District Court*, 407 U.S. 297, 313-14 (1972).

[5]407 U.S. at 299.

[6]*Id.*, at 391-321. Justice Powell also observed that,

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961).... Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." . . . .

powers, within or without the country."[7] The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents."[8] However, the guidance which the Court provided in *Keith* with respect to national security surveillance in a domestic context to some degree presaged the approach Congress was to take in foreign intelligence surveillance. The *Keith* Court observed in part:

> . . . We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crimes. Given these potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. . . . It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . .; and that the time and reporting requirements need not be so strict as those in § 2518. The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.[9]

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of Brown, an American citizen, was incidentally overheard. The Third Circuit in *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom, Ivanov v.*

---

[7] *Id.*, at 308.

[8] *Id.*, at 321-22.

[9] 407 U.S. at 323-24.

United States, 419 U.S. 881 (1974), concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information. In its plurality decision in *Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976), the District of Columbia Circuit took a somewhat different view in a case involving a warrantless wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power. Finding that a warrant was required in such circumstances, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."

With the passage of the Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified as amended at 50 U.S.C. § 1801 *et seq.*, Congress sought to strike a delicate balance between these interests when the gathering of foreign intelligence involved the use of electronic surveillance.[10] Collection of foreign intelligence information through electronic surveillance is now governed by FISA and E.O. 12333.[11] This report will examine the provisions of FISA which deal with electronic surveillance, in the foreign intelligence context, as well as those applicable to physical searches, the use of pen registers and trap and trace devices under FISA, and access to business records and other tangible things for foreign intelligence purposes. As the provisions of E.O. 12333 to some extent set the broader context within which FISA operates, we will briefly examine its pertinent provisions first.

Executive Order 12333

Under Part 2.3 of E.O. 12333, the agencies within the Intelligence Community are to "collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. . . ." Among the types of information that can be collected, retained or disseminated under this section are:

> (a) Information that is publicly available or collected with the consent of the person concerned;

---

[10]For an examination of the legislative history of P.L. 95-511, see S. Rept. 95-604, Senate Committee on the Judiciary, Parts I and II (Nov. 15, 22, 1977); S. Rept. 95-701, Senate Select Committee on Intelligence (March 14, 1978); H. Rept. 95-1283, House Permanent Select Committee on Intelligence (June 8, 1978); H. Conf. Rept. 95-1720 (Oct. 5, 1978); Senate Reports and House Conference Report are reprinted in 1978 *U.S. Code Cong. & Admin. News* 3904.

[11] Physical searches for foreign intelligence information are governed by 50 U.S.C. § 1821 *et seq.*, while the use of pen registers and trap and trace devices in connection with foreign intelligence investigations is addressed in 50 U.S.C. § 1841 *et seq.* Access to certain business records for foreign intelligence or international terrorism investigative purposes is covered by 50 U.S.C. § 1861 *et seq.*

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical or communications security investigation;

. . .

(i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

In discussing collections techniques, Part 2.4 of E.O. 12333 indicates that agencies within the Intelligence Community are to use

the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. . . .

Part 2.5 of the Executive Order 12333 states that:

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for

law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978 [section 1801 et seq. of this title], shall be conducted in accordance with that Act, as well as this Order.

The Foreign Intelligence Surveillance Act

The Statutory Framework

Electronic surveillance under FISA. The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, as amended, provides a framework for the use of electronic surveillance,[12] physical searches, pen registers and trap and trace devices to acquire foreign intelligence information.[13] This measure seeks to strike a balance

---

[12]50 U.S.C. § 1801(f)(2) defines "electronic surveillance" to mean:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any person thereto, if such acquisition occurs in the United States, *but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18*;
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

The italicized portion of Subsection 1801(f)(2) was added by Sec. 1003 of P.L. 107-56.

[13]"Foreign intelligence information" is defined in 50 U.S.C. § 1801(e) to mean:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power;

(continued...)

between national security needs in the context of foreign intelligence gathering and privacy rights.

Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance to acquire foreign intelligence information for up to one year without a court order if two criteria are satisfied. First, to utilize this authority, the Attorney General must certify in writing under oath that:

> (A) the electronic surveillance is solely directed at —
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2) or (3) of this title;
> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
> (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title;[14]

---

[13](...continued)

> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
> (A) the national defense or the security of the United States; or
> (B) the conduct of the foreign affairs of the United States.

"International terrorism" is defined in 50 U.S.C. § 1801(c) to mean activities that:

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
>
> (2) appear to be intended–
> (A) to intimidate or coerce a civilian population;
> (B) to influence the policy of a government by intimidation or coercion; or
> (C) to affect the conduct of a government by assassination or kidnapping; and
> (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

"Sabotage" is defined in 50 U.S.C. § 1801(d) to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States."

[14]Minimization procedures with respect to electronic surveillance are defined in 50 U.S.C. § 1801(h) to mean:

(continued...)

[14](...continued)

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Sec. 314(a)(1) of H. Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002 to accompany H.R. 2883, amended 50 U.S.C. § 1801(h)(4) to change to 72 hours what was previously a 24 hour period beyond which the contents of any communication to which a U.S. person is a party may not be retained absent a court order under 50 U.S.C. § 1805 or a finding by the Attorney General that the information indicates a threat of death or serious bodily injury. The conference version of H.R. 2883 received the approbation of both houses of Congress, and was forwarded to the President on December 18, 2001, for his signature. It became P.L. 107-108.

"United States person" is defined in 50 U.S.C. § 1801(i) to mean

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

"Foreign power" is defined in 50 U.S.C. § 1801(a) to mean:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(continued...)

. . . .

Second, in order for the President, through the Attorney General, to use this authority

> . . . the Attorney General [must report] such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization and the reason for their becoming effective immediately.

---

[14](...continued)

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

"Agent of a foreign power" is defined in 50 U.S.C. § 1801(b) to mean:

> (1) any person other than a United States person, who--
>
> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;
>
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
>
> (2) any person who--
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Such electronic surveillance must be conducted only in accordance with the Attorney General's certification and minimization procedures adopted by him. A copy of his certification must be transmitted by the Attorney General to the court established under 50 U.S.C. § 1803(a) (hereinafter the FISC).[15] This certification remains under seal unless an application for a court order for surveillance authority is made under 50 U.S.C. §§ 1801(h)(4) and 1804,[16] or the certification is necessary to determine the legality of the surveillance under 50 U.S.C. § 1806(f).[17] 50 U.S.C. § 1802(a)(2) and (a)(3).

In connection with electronic surveillance so authorized, the Attorney General may direct a specified communications common carrier to furnish all information, facilities, or technical assistance needed for the electronic surveillance to be accomplished in a way that would protect its secrecy and minimize interference with the services provided by the carrier to its customers. 50 U.S.C. § 1802(a)(4)(A). In addition, the Attorney General may direct the specified communications common carrier to maintain any records, under security procedures approved by the Attorney General and the Director of Central Intelligence, concerning the surveillance or the assistance provided which the carrier wishes to retain. 50 U.S.C. § 1802(a)(4)(B). Compensation at the prevailing rate must be made to the carrier by the Government for providing such aid.

If the President, by written authorization, empowers the Attorney General to approve applications to the FISC, an application for a court order may be made pursuant to 50 U.S.C. § 1802(b). A judge receiving such an application may grant an order under 50 U.S.C. § 1805 approving electronic surveillance of a foreign power or an agent of a foreign power to obtain foreign intelligence information. There is an exception to this, however. Under 50 U.S.C. § 1802(b), a court does not have jurisdiction to grant an order approving electronic surveillance directed solely as

---

[15]Under 50 U.S.C. § 1803(a), as amended by Section 208 of P.L. 107-56, the Chief Justice of the United States must publicly designate eleven U.S. district court judges from seven of the United States judicial circuits, of whom no fewer than three must reside within 20 miles of the District of Columbia. These eleven judges constitute the court which has jurisdiction over applications for and orders approving electronic surveillance anywhere within the Unite States under FISA. If an application for electronic surveillance under this Act is denied by one judge of this court, it may not then be considered by another judge on the court. If a judge denies such an application, he or she must immediately provide a written statement for the record of the reason(s) for this decision. If the United States so moves, this record must then be transmitted under seal to a court of review established under 50 U.S.C. § 1803(b). The Chief Justice also publicly designates the three U.S. district court or U.S. court of appeals judges who together make up the court of review having jurisdiction to review any denial of an order under FISA. If that court determines that an application was properly denied, again a written record of the reason(s) for the court of review's decision must be provided for the record, and the United States may petition for a writ of certiorari to the United States Supreme Court. All proceedings under this Act must be conducted expeditiously, and the record of all proceedings including applications and orders granted, must be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of Central Intelligence. 50 U.S.C. § 1803(c).

[16]50 U.S.C. § 1804 is discussed at pages 11-15 of this report, *infra.*

[17]50 U.S.C. § 1806 is discussed at pages 20-25 of this report, *infra.*

described in 50 U.S.C. § 1802(a)(1)(A) (that is, at acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, or acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power), unless the surveillance may involve the acquisition of communications of a United States person. 50 U.S.C. § 1802(b).

An application for a court order authorizing electronic surveillance for foreign intelligence purposes may be sought under 50 U.S.C. § 1804. An application for such a court order must be made by a federal officer in writing on oath or affirmation to an FISC judge. The application must be approved by the Attorney General based upon his finding that the criteria and requirements set forth in 50 U.S.C. § 1801 *et seq.* have been met. Section 1804(a) sets out what must be included in the application:

> (1) the identity of the Federal officer making the application;
> (2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;
> (3) the identity, if known, or a description of the target of the electronic surveillance;
> (4) a statement of the facts and circumstances relied upon by the applicant to justify his belief that —
>
> (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and
>
> (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (5) a statement of the proposed minimization procedures;
> (6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
> (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate[18]—
>
> (A) that the certifying official deems the information sought to be foreign intelligence information;

[18]Under Section 1-103 of Executive Order 12139, the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the FBI, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence were designated to make such certifications in support of applications to engage in electronic surveillance for foreign intelligence purposes. Neither these officials nor anyone acting in those capacities may make such certifications unless they are appointed by the President with the advice and consent of the Senate.

(B) that *a significant*[19] purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in 1801(e) of this title; and

(E) including a statement of the basis for the certification that —

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

---

[19] Section 218 of P.L. 107-56 amended the requisite certifications to be made by the Assistant to the President for National Security Affairs, or other designated official (see footnote 18). Heretofore, the certifying official had to certify, among other things, that *the* purpose of the electronic surveillance under FISA was to obtain foreign intelligence information. Under the new language, the certifying official must certify that *a significant* purpose of such electronic surveillance is to obtain foreign intelligence information. This change may have the effect of somewhat blurring the line between electronic surveillance for foreign intelligence purposes and that engaged in for criminal law enforcement purposes.

Past cases considering the constitutional sufficiency of FISA in the context of electronic surveillance have rejected Fourth Amendment challenges and due process challenges under the Fifth Amendment to the use of information gleaned from a FISA electronic surveillance in a subsequent criminal prosecution, because the purpose of the FISA electronic surveillance, both initially and throughout the surveillance, was to secure foreign intelligence information and not primarily oriented towards criminal investigation or prosecution, *United States v. Megahey*, 553 F. Supp. 1180, 1185-1193 (D.N.Y.), *aff'd* 729 F.2d 1444 (2d Cir. 1982); *United States v. Ott*, 827 F.2d 473, 475 (9th Cir. 1987); *United States. v Badia*, 827 F. 2d 1458, 1464 (11th Cir. 1987). *See also*, *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991), *rehearing and cert. denied*, 506 U.S. 816 (1991) (holding that, although evidence obtained in FISA electronic surveillance may later be used in a criminal prosecution, criminal investigation may not be the primary purpose of the surveillance, and FISA may not be used as an end-run around the 4th Amendment); *United States v. Pelton*, 835 F.2d 1067, 1074-76 (4th Cir. 1987), *cert. denied*, 486 U.S.1010 (1987) (holding that electronic surveillance under FISA passed constitutional muster where primary purpose of surveillance, initially and throughout surveillance, was gathering of foreign intelligence information; also held that an otherwise valid FISA surveillance was not invalidated because later use of the fruits of the surveillance in criminal prosecution could be anticipated. In addition, the court rejected Pelton's challenge to FISA on the ground that allowing any electronic surveillance on less than the traditional probable cause standard–i.e. probable cause to believe the suspect has committed, is committing, or is about to commit a crime for which electronic surveillance is permitted, and that the interception will obtain communications concerning that offense--for issuance of a search warrant was violative of the 4th Amendment, finding FISA's provisions to be reasonable both in relation to the legitimate need of Government for foreign intelligence information and the protected rights of U.S. citizens); *United States v. Rahman*, 861 F. Supp. 247, 251 (S.D. N.Y. 1994). *Cf., United States v. Bin Laden*, 2001 U.S. Dist. LEXIS 15484 (S.D. N.Y., October 2, 2001); *United States v. Bin Laden*, 126 F. Supp. 264, 277-78 (S.D. N.Y. 2000) (adopting foreign intelligence exception to the warrant requirement for searches targeting foreign powers or agents of foreign powers abroad; noting that this "exception to the warrant requirement applies until and unless the primary purpose of the searches stops being foreign intelligence collection. . . . If foreign intelligence collection is merely *a* purpose and not the *primary* purpose of a search, the exception does not apply.")

(8) a statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application;

(10) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter; and

(11) whenever more that one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device.

The application for a court order need not contain the information required in Subsections 1804(6), (7)(E), (8), and (11) above if the target of the electronic surveillance is a foreign power and each of the facilities or places at which surveillance is directed is owned, leased, or exclusively used by that foreign power. However, in those circumstances, the application must indicate whether physical entry is needed to effect the surveillance, and must also contain such information about the surveillance techniques and communications or other information regarding United States persons likely to be obtained as may be necessary to assess the proposed minimization procedures. 50 U.S.C. § 1804(b).

Where an application for electronic surveillance under 50 U.S.C. § 1804(a) involves a target described in 50 U.S.C. § 1801(b)(2),[20] the Attorney General must personally review the application if requested to do so, in writing, by the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of Central Intelligence.[21] The authority to make such a request may not be delegated unless the official involved is disabled or otherwise unavailable.[22] Each such official must make appropriate arrangements, in advance, to ensure that such a delegation of authority is clearly established in case of disability or other unavailability.[23] If the Attorney General determines that an application should not be approved, he must give the official requesting the Attorney General's personal review of the application written notice of the determination. Except in cases where the Attorney General is disabled or otherwise unavailable, the responsibility for such a determination may not be delegated. The Attorney General must make advance plans to ensure that the delegation of such responsibility where the Attorney General is disabled or otherwise unavailable is clearly established.[24] Notice of the Attorney General's determination that an application should not be approved must indicate

---

[20]For a list of those covered in 50 U.S.C. § 1801(b)(2), see footnote 14, *supra.*

[21]50 U.S.C. § 1804(e)(1)(A).

[22]50 U.S.C. § 1804(e)(1)(B).

[23]50 U.S.C. § 1804(e)(1)(C).

[24]50 U.S.C. § 1804(e)(2)(A).

what modifications, if any, should be made in the application needed to make it meet with the Attorney General's approval.[25] The official receiving the Attorney General's notice of modifications which would make the application acceptable must modify the application if the official deems such modifications warranted. Except in cases of disability or other unavailability, the responsibility to supervise any such modifications is also a non-delegable responsibility.[26]

If a judge makes the findings required under 50 U.S.C. § 1805(a), then he or she must enter an ex parte order as requested or as modified approving the electronic surveillance. The necessary findings must include that:

> (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
> (2) the application has been made by a Federal officer and approved by the Attorney General;
> (3) on the basis of the facts submitted by the applicant there is probable cause to believe that —
> (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
> (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
> (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and
> (5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

In making a probable cause determination under 50 U.S.C. § 1805(a)(3), the judge may consider past activities of the target as well as facts and circumstances relating to the target's current or future activities.[27] An order approving an electronic surveillance under Section 1805(c) must:

> (1) specify–
> (A) the identity, if known, or a description of the target of the electronic surveillance;
> (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, *if known*;[28]

---

[25]50 U.S.C. § 1804(e)(2)(B).

[26]50 U.S.C. § 1804(e)(2)(C).

[27]50 U.S.C. § 1805(b).

[28]Section 314(a)(2)(A) of H. Rept. 107-328, the conference report on the Intelligence Authorization Act for Fiscal Year 2002, to accompany H.R. 2883, added "if known" to the

(continued...)

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(E) the period of time during which the electronic surveillance is approved; and

(F) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the device involved and what minimization procedures shall apply to information subject to acquisition by each device; and

(2) direct–

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant a specified communication or other common carrier, landlord, custodian, or other specified person, *or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,* furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.[29]

The italicized portions of Section 1805(c)(1)(B) and Section1805(c)(2)(B) reflect changes, added by P.L. 107-108 and P.L. 107-56 respectively, intended to provide authority for "multipoint" or "roving" electronic surveillance where the actions of the target of the surveillance, such as switching phones and locations repeatedly, may thwart that surveillance. The Conference Report on H.R. 2338, the Intelligence Authorization Act for Fiscal Year 2002, H. Rept. 107-328, at page 24, provided the following explanation of these changes:

> The multipoint wiretap amendment to FISA in the USA PATRIOT Act (section 206) allows the FISA court to issue generic orders of assistance to any

---

[28](...continued)
end of Section 1805(c)(1)(B) before the semi-colon. The conference version of the bill passed both the House and the Senate, and was signed by the President on December 28, 2001.

[29]50 U.S.C. § 1805(c). The italics in 50 U.S.C. § 1805(c)(2)(B), above, indicates new language added by Section 206 of P.L. 107-56. Where circumstances suggest that a target's actions may prevent identification of a specified person, this new language appears to permit the Foreign Intelligence Surveillance Court to require a service provider, other common carrier, landlord, custodian or other persons to provide necessary assistance to the applicant for a FISA order for electronic surveillance. The heading to Section 6 of P.L. 107-56 refers to this as "roving surveillance authority." H. Rept. 107-328 calls this a "multipoint" wiretap. *Intelligence Authorization Act for Fiscal Year 2002*, 107th Cong., 1st Sess., H. Rept. 107-328, Conference Report, at 24 (Dec. 6, 2001).

> communications provider or similar person, instead of to a particular communications provider. This change permits the Government to implement new surveillance immediately if the FISA target changes providers in an effort to thwart surveillance. The amendment was directed at persons who, for example, attempt to defeat surveillance by changing wireless telephone providers or using pay phones.
>
> Currently, FISA requires the court to "specify" the "nature and location of each of the facilities or places at which the electronic surveillance will be directed." 50 U.S.C. § 105(c)(1)(B). Obviously, in certain situations under current law, such a specification is limited. For example, a wireless phone has no fixed location and electronic mail may be accessed from any number of locations.
>
> To avoid any ambiguity and clarify Congress' intent, the conferees agreed to a provision which adds the phrase, "if known," to the end of 50 U.S.C. § 1805(c)(1)(B). The "if known" language, which follows the model of 50 U.S.C. § 1805(c)(1)(A), is designed to avoid any uncertainty about the kind of specification required in a multipoint wiretap case, where the facility to be monitored is typically not known in advance.

If the target of the electronic surveillance is a foreign power and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the order does not need to include the information covered by Section 1805(c)(1)(C), (D), and (F), but must generally describe the information sought, the communications or activities subject to surveillance, the type of electronic surveillance used, and whether physical entry is needed. 50 U.S.C. § 1805(d).

Such an order may approve an electronic surveillance for the period of time necessary to achieve its purpose or for ninety days, whichever is less, unless the order is targeted against a foreign power. In that event, the order shall approve an electronic surveillance for the period specified in the order or for one year, whichever is less. An order under FISA for surveillance targeted against an agent of a foreign power who acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor, may be for the period specified in the order or 120 days, whichever is less.[30] Generally, upon application for an extension, a court may grant an extension of an order on the same basis as an original order. An extension must include new findings made in the same manner as that required for the original order. However, an extension of an order for a surveillance targeting a foreign power that is not a United States person may be for a period of up to one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period involved. In addition, an extension of an order for surveillance targeted at an agent of a foreign power who acts in the United States as an officer or employee of a foreign power or as a member of a group engaged in international terrorism or activities in preparation therefore may be extended to a period not exceeding one year. 50 U.S.C. § 1805(e)(2)(A) and (B).[31]

---

[30]50 U.S.C. § 1805(e)(1)(B), as added by Section 207 of P.L. 107-56.

[31]Section 207 of P.L. 107-56 appears to have included a mistaken citation here, referring to (continued...)

Emergency situations are addressed in 50 U.S.C. § 1805(f).[32] Notwithstanding other provisions of this subchapter, if the Attorney General reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained and that the factual basis for issuance of an order under this subchapter to approve such surveillance exists, he may authorize electronic surveillance if specified steps are taken. At the time of the Attorney General's emergency authorization, he or his designee must inform an FISC judge that the decision to employ emergency electronic surveillance has been made. An application for a court order under Section 1804 must be made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes emergency electronic surveillance, he must require compliance with the minimization procedures required for the issuance of a judicial order under this subchapter. Absent a judicial order

---

[31](...continued)
50 U.S.C. § *1805(d)(2)* instead of 50 U.S.C. § *1805(e)(2)* (emphasis added). The amending statutory language discussed above appears to reflect an intended change to subsection 1805(e)(2), as there is no existing statutory language readily susceptible to such an amendment in subsection 1805(d)(2). Section 314(c)(1) of P.L. 107-108, the conference version of H.R. 2883, in H. Rept. 107-328, corrected the apparent error from P.L. 107-56, Section 207, so that the reference is now to 50 U.S.C. § 1805(e)(2). The conference version of H.R. 2883 was signed into law by the President on December 28, 2001.

[32]50 U.S.C. § 1805(g) authorizes officers, employees, or agents of the United States to conduct electronic surveillance in the normal course of their official duties to test electronic equipment, determine the existence and capability of equipment used for unauthorized electronic surveillance, or to train intelligence personnel in the use of electronic surveillance equipment. Under 50 U.S.C. § 1805(h), the certifications of the Attorney General pursuant to 50 U.S.C. § 1802(a) and applications made and orders granted for electronic surveillance under FISA must be retained for at least 10 years.

Section 225 of P.L. 107-56 appears to create a second subsection 1805(h), which precludes any cause of action in any court "against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance" under FISA. This immunity provision is included in 50 U.S.C. § 1805, and was denominated "Immunity for Compliance with FISA Wiretap" in Section 225 of the USA PATRIOT Act, both facts which might lead one to conclude that it applied only to electronic surveillance under FISA. However, in H.Rept. 107-328, the conference report accompanying H.R. 2883, which became P.L. 107-108, the conferees expressed the view that "the text of section 225 refers to court orders and requests for emergency assistance 'under this Act,' which makes clear that it applies to physical searches (and pen-trap requests–for which there already exists an immunity provision, 50 U.S.C. § 1842(f)–and subpoenas) as well as electronic surveillance." *Id.* at 25.

Section 314(a)(2)(C) of P.L. 107-108, the conference report version of H.R. 2883, in H. Rept. 107-328, changed subsection (h), which was added to 50 U.S.C. § 1805 by Section 225 of P.L. 107-56, to subsection (i). In addition, Section 314(a)(2)(D) of the conference report version of H.R. 2883 added "for electronic surveillance or physical search" to the end of the newly designated 50 U.S.C. § 1805(i) before the final period. The measure was signed into law by the President on December 28, 2001.

approving the emergency electronic surveillance, the surveillance must terminate when the information sought is obtained, when the application for the order is denied, or after 72 hours from the time of the Attorney General's authorization, whichever is earliest.[33] If no judicial order approving the surveillance is issued, the information garnered may not be received in evidence or otherwise disclosed in any court proceeding, or proceeding in or before any grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof. No information concerning any United States person acquired through such surveillance may be disclosed by any Federal officer or employee without the consent of that person, unless the Attorney General approves of such disclosure or use where the information indicates a threat of death or serious bodily harm to any person.[34]

---

[33]Section 314(a)(2)(B) of the conference report version of H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002, H. Rept. 107-328, replaced 24 hours with 72 hours in each place that it appears in 50 U.S.C. § 1805(f). The measure was forwarded to the President for his signature on December 18, 2001, and signed into law on December 28, 2001, as P.L. 107-108.

[34]Some of the provisions dealing with interception of wire, oral, or electronic communications in the context of criminal law investigations, 18 U.S.C. §§ 2510 *et seq.*, may also be worthy of note. With certain exceptions, these provisions, among other things, prohibit any person from engaging in intentional interception; attempted interception; or procuring others to intercept or endeavor to intercept wire, oral, or electronic communication; or intentional disclosure; attempting to disclose; using or endeavoring to use the contents of a wire, oral or electronic communication, knowing or having reason to know that the information was obtained by such an unlawful interception. 18 U.S.C. § 2511. "Person" is defined in 18 U.S.C. § 2510(6) to include "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." Among the exceptions to Section 2511 are two of particular note:

> (2)(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.
>
> (2)(f) Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

Among other things, Section 2512 prohibits any person from intentionally manufacturing, assembling, possessing, or selling any electronic, mechanical, or other device, knowing that its design renders it primarily useful for the purpose of the

(continued...)

[34](...continued)
surreptitious interception of wire, oral, or electronic communications and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce. It also prohibits any person from intentionally sending such a device through the mail or sending or carrying such a device in interstate or foreign commerce, knowing that such surreptitious interception is its primary purpose. Similarly, intentionally advertising such a device, knowing or having reason to know that the advertisement will be sent through the mail or transported in interstate or foreign commerce is foreclosed. Again an exception to these general prohibitions in Section 2512 may be of particular interest:

> (2) It shall not be unlawful under this section for—
> (a) . . .
> (b) an officer, agent, or employee of, or a person under contract with, the United States . . . in the normal course of the activities of the United States . . .,
> to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

In addition, Section 107 of the Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1858, October 21, 1986, [which enacted 18 U.S.C. §§ 1367, 2621, 2701 to 2711, 3117, and 3121 to 3126; and amended 18 U.S.C. §§ 2232, 2511-2513, and 2516-2520], provided generally that, "[n]othing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity." It also stated:

> (b) Certain Activities Under Procedures Approved by the Attorney General.–Nothing in chapter 119 [interception of wire, oral or electronic communications] or chapter 121 [stored wire and electronic communications and transactional records access] of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to--
> (1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;
> (2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.]; or
> (3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978 [50 U.S.C. § 1801 et seq.].

In addition, Chapter 121 of title 18 of the United States Code deals with stored wire and electronic communications and transactional records. Under 18 U.S.C. § 2701, intentionally accessing without authorization a facility through which an electronic communication service is provided, or intentionally exceeding an authorization to access such a facility and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage in such system is prohibited. Upon compliance with statutory requirements in 18 U.S.C. § 2709, the Director of the FBI
(continued...)

The uses to which information gathered under FISA may be put are addressed under 50 U.S.C. § 1806.[35] Under these provisions, disclosure, without the

---

[34](...continued)
or his designee in a position not lower than deputy Assistant Director may seek access to telephone toll and transactional records for foreign counterintelligence purposes. The FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the FBI, and, "with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency." 18 U.S.C. § 2709(d).

[35]The provisions of Section 1806 are as follows:

> (a) Compliance with minimization procedures; privileged communications; lawful purposes
>
> Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with or in violation of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.
>
> (b) Statement for disclosure
>
> No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.
>
> (c) Notification by United States
>
> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.
>
> (d) Notification by States or political subdivisions
>
> Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof intends to so disclose or so use such information.
>
> (e) Motion to suppress
>
> Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced

(continued...)

[35](...continued)

or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio

(continued...)

consent of the person involved, of information lawfully acquired under FISA which concerns a United States person must be in compliance with the statutorily mandated minimization procedures. Communications which were privileged when intercepted remain privileged. Where information acquired under FISA is disclosed for law enforcement purposes, neither that information nor any information derived therefrom may be used in a criminal proceeding without prior authorization of the Attorney General. If the United States Government intends to disclose information acquired under FISA or derived therefrom in any proceeding before a court, department, officer

---

[35](...continued)

communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application or on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forgo ordering the serving of the notice required under this subsection.

(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against–

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) [50 U.S.C. § 1804(a)(7)(B) (referring to a certification by the Assistant to the President for National Security Affairs or other designated certifying authority "that a significant purpose of the surveillance is to obtain foreign intelligence information")] or the entry of an order under section 105 [50 U.S.C. § 1805].

Subsection 1806(k) was added by Section 504 of P.L. 107-56. The term "aggrieved person," as used in connection with electronic surveillance under FISA, is defined under 50 U.S.C. § 1801(k) to mean "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."

regulatory body or other authority of the United States against an aggrieved person,[36] then the Government must give prior notice of its intent to disclose to the aggrieved person and to the court or other authority involved. Similarly, a State or political subdivision of a State that intends to disclose such information against an aggrieved person in a proceeding before a State or local authority must give prior notice of its intent to the aggrieved person, the court or other authority, and the Attorney General.

Section 1806 also sets out in camera and ex parte district court review procedures to be followed where such notification is received, or where the aggrieved person seeks to discover or obtain orders or applications relating to FISA electronic surveillance, or to discover, obtain, or suppress evidence or information obtained or derived from the electronic surveillance, and the Attorney General files an affidavit under oath that such disclosure would harm U.S. national security. The focus of this review would be to determine whether the surveillance was lawfully conducted and authorized. Only where needed to make an accurate determination of these issues does the section permit the court to disclose to the aggrieved person, under appropriate security measures and protective orders, parts of the application, order, or other materials related to the surveillance. If, as a result of its review, the district court determines that the surveillance was unlawful, the resulting evidence must be suppressed.[37] If the surveillance was lawfully authorized and conducted, the motion

---

[36]For the definition of "aggrieved person" as that term is used with respect to targets of electronic surveillance under FISA, see fn. 35, *supra*.

[37]*But see, United States v. Thomson*, 752 F. Supp. 75, 77 (W.D. N.Y. 1990), stating that,

> If the Court determines that the surveillance was unlawfully authorized or conducted, it must order disclosure of the FISA material. 50 U.S.C. § 1806(g) .... In *United States v. Belfield*, 692 F.2d 141 (D.C. Cir. 1982), the court stated that: "even when the government has purported not to be offering any evidence obtained or derived from the electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the FISA surveillance material to ensure that no fruits thereof are being used against him." Id. at 146.

It may be noted that the Section 1806(g) does not state that a court must order disclosure of the FISA material if the court finds that the FISA electronic surveillance was unlawfully authorized or conducted. Rather, the provision in question states in pertinent part that, "If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. . . ." While a district court will normally consider in camera and ex parte a motion to suppress under Subsection 1806(e) or other statute or rule to discover, disclose, or suppress information relating to a FISA electronic surveillance, Subsection 1806(f) does permit a district court, in determining the legality of a FISA electronic surveillance, to disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance only to the extent necessary to make an accurate determination of the legality of the surveillance. *Belfield* indicated that a criminal defendant may seek to discover FISA surveillance material to ensure that no fruits of an illegal surveillance are

(continued...)

of the aggrieved person must be denied except to the extent that due process requires discovery or disclosure. Resultant court orders granting motions or requests of the aggrieved person for a determination that the surveillance was not lawfully conducted or authorized and court orders requiring review or granting disclosure are final orders binding on all Federal and State courts except a U.S. Court of Appeals and the U.S. Supreme Court.

If the contents of any radio communication are unintentionally acquired by an electronic, mechanical, or other surveillance device in circumstances where there is a reasonable expectation of privacy and where a warrant would be required if the surveillance were to be pursued for law enforcement purposes, then the contents must be destroyed when recognized, unless the Attorney General finds that the contents indicate a threat of death or serious bodily harm to any person.

As noted above, Section 1805 provides for emergency electronic surveillance in limited circumstances, and requires the subsequent prompt filing of an application for court authorization to the FISC in such a situation. Under Section 1806, if the application is unsuccessful in obtaining court approval for the surveillance, notice must be served upon any United States person named in the application and such other U.S. persons subject to electronic surveillance as the judge determines, in the exercise of his discretion, is in the interests of justice. This notice includes the fact of the application, the period of surveillance, and the fact that information was or was not obtained during this period. Section 1806 permits postponement or suspension of service of notice for up to ninety days upon ex parte good cause shown. Upon a further ex parte showing of good cause thereafter, the court will forego ordering such service of notice.[38]

---

[37](...continued)
being used against him, but it appears to stop short of saying that in every instance where the court finds an illegal surveillance disclosure must be forthcoming. "The language of section 1806(f) clearly anticipates that an ex parte, in camera determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary." *Belfield, supra*, 692 F.2d at 147. *See also, United States v. Squillacote*, 221 F.3d 542, 552-554 (4th Cir. 2000), *cert. denied*, ___ U.S. ___, 2001 U.S. LEXIS 2915 (April 16, 2001).

[38] *Cf., United States Attorney's Manual*, §§ 1-2.106 (Office of Intelligence Policy and Review organization and functions). This section indicates, in part, that the Office of Intelligence Policy and Review

> . . . prepares certifications and applications for electronic surveillance under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq., and represents the United States before the United States Foreign Intelligence Surveillance Court. It processes requests for Attorney General Authority to use FISA material in adjudicatory proceedings and assists in responding to challenges to the legality of FISA surveillances.

See also, 28 C.F.R. § 0.33 (functions of the Counsel for Intelligence Policy);*United States Attorneys' Criminal Resource Manual*, §§ 1073 (FISA–50 U.S.C. § 1809) and 1075 (elements of the offense under 50 U.S.C. § 1809(a)); *cf., United States Attorney's Manual* § 9-7.301 (consensual monitoring in the context of electronic surveillance).

P.L. 107-56, Section 504, added a new subsection 1806(k)(1). Under this new subsection, federal officers who conduct electronic surveillance to acquire foreign intelligence under FISA are permitted to consult with Federal law enforcement officers to coordinate investigative efforts or to protect against–

> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

This new subsection indicates further that such coordination would not preclude certification as required by 50 U.S.C. § 1804(a)(7)(B) or entry of a court order under 50 U.S.C. § 1805.

Reporting requirements are included in Sections 1807 and 1808. Under Section 1807, each year in April, the Attorney General is directed to transmit to the Administrative Office of the United States Courts and to the Congress a report covering the total number of applications made for orders and extensions of orders approving electronic surveillance under FISA during the previous year, and the total number of orders and extensions granted, modified, or denied during that time period. Section 1808(a) requires the Attorney General to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence semiannually about all electronic surveillance under FISA.[39] Each such report must contain a description of each criminal case in which information acquired under FISA "has been passed for law enforcement purposes" during the period covered by the report, and each criminal case in which information acquired under FISA has been authorized to be used at trial during the reporting period.[40]

Section 1809 provides criminal sanctions for intentionally engaging in electronic surveillance under color of law except as authorized by statute; or for disclosing or using information obtained under color of law by electronic surveillance, knowing or having reason to know that surveillance was not authorized by statute.[41] The

---

[39]Subsection 1808(b) directed these committees to report annually for five years after the date of enactment to the House and the Senate respectively concerning implementation of FISA, including any recommendations for amendment, repeal, or continuation without amendment. P.L. 106-567, Title VI, Sec. 604(b) (Dec. 27, 2000), 114 Stat. 2853, required the Attorney General to submit to the Senate Select Committee on Intelligence, the Senate Judiciary Committee, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee a report on the authorities and procedures utilized by the Department of Justice to determine whether or not to disclose information acquired under FISA for law enforcement purposes. 50 U.S.C. § 1806 note.

[40]50 U.S.C. § 1808(a)(2).

[41]Section 1075 of the *United States Attorneys' Criminal Resource Manual* indicates that Section 1809(a) "reaches two distinct acts: (1) engaging in unauthorized electronic surveillance under color of law; and (2) using or disclosing information obtained under color of law through unauthorized electronic surveillance. Each offense involves an "intentional"

(continued...)

provision makes it a defense to prosecution under this subsection if the defendant is a law enforcement officer or investigative officer in the course of his official duties and the electronic surveillance was authorized by and conducted under a search warrant or court order of a court of competent jurisdiction. Section 1809 provides for Federal jurisdiction over such an offense if the defendant is a Federal officer or employee at the time of the offense. Civil liability is also provided for under Section 1810, where an aggrieved person, who is neither a foreign power nor an agent of a foreign power, has been subjected to electronic surveillance, or where information gathered by electronic surveillance about an aggrieved person has been disclosed or used in violation of Section 1809.

Finally, Section 1811 provides that, notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order to acquire foreign intelligence information for up to 15 calendar days following a declaration of war by Congress.

Physical searches for foreign intelligence gathering purposes. Physical searches for foreign intelligence purposes are addressed in 50 U.S.C. § 1821 *et seq.*[42] While tailored for physical searches, the provisions in many respects follow a pattern similar to that created for electronic surveillance. The definitions from 50 U.S.C. § 1801 for the terms "foreign power," "agent of a foreign power," "international terrorism," "sabotage," "foreign intelligence information," "Attorney General," "United States person," "United States," "person," and "State" also apply to foreign intelligence physical searches except where specifically provided otherwise. A "physical search" under this title means:

> any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 1801(f) of this title [50 U.S.C.], or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in

---

[41](...continued)
state of mind and unauthorized "electronic surveillance." Section 1075 further notes:

> Even though none of these elements mentions foreign intelligence, one court has explained that "the FISA applies only to surveillance designed to gather information relevant to foreign intelligence." *United States v. Koyomejian*, 970 F. 2d 536, 540 (9th Cir. 1992) (en banc), cert denied, 506 U.S. 1005 (1992). In fact, all applications for an order from the Foreign Intelligence Surveillance Court require a certification from a presidentially designated official that the purpose of the surveillance is to obtain foreign intelligence. 50 U.S.C. § 1804(a)(7).

[42]The physical search provisions of FISA were added as Title III of that Act by P.L. 103-359, Title VIII, on October 14, 1994, 108 Stat. 3443. Some of these provisions were subsequently amended by P.L. 106-567, Title VI, on December 27, 2000, 114 Stat. 2852-53; and by P.L. 107-56.

> accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 1801(f) of this title.[43]

Minimization procedures also apply to physical searches for foreign intelligence purposes. Those defined under 50 U.S.C. § 1821(4) are tailored to such physical searches, and like those applicable to electronic surveillance under 50 U.S.C. § 1801(h), these procedures are designed to minimize acquisition and retention, and to prohibit dissemination of nonpublicly available information concerning unconsenting U.S. persons, consistent with the needs of the United States to obtain, produce and disseminate foreign intelligence.[44]

Under 50 U.S.C. § 1822, the President, acting through the Attorney General may authorize physical searches to acquire foreign intelligence information without a court order for up to one year if the Attorney General certifies under oath that the search is solely directed at premises, property, information or materials owned by or under the open and exclusive control of a foreign power or powers.[45] For these purposes,

---

[43]50 U.S.C. § 1821(5).

[44]Specifically, 50 U.S.C. § 1821(4) defines "minimization procedures" with respect to physical search to mean:

> (A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> (B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand such foreign intelligence information or assess its importance;
> (C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
> (D) notwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 1822(a) of this title, procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours, unless a court order under section 1824 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Section 314(a)(3) of P.L. 107-108, the conference version of the Intelligence Authorization Act of 2002, H.R. 2883, from H. Rept. 107-328, changed the previous 24 hour period in the minimization procedures under 50 U.S.C. § 1821(4)(D) to a 72 hour period. The bill passed both houses of Congress and was signed by the President on December 28, 2001.

[45]The president provided such authority to the Attorney General by Executive Order 12949, (continued...)

"foreign power or powers" means a foreign government or component of a foreign government, whether or not recognized by the United States, a faction of a foreign nation or nations, not substantially composed of U.S. persons; or an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.[46] In addition, the Attorney General must certify that there is no substantial likelihood that the physical search will involve the premises, information, material or property of a U.S. person, and that the proposed minimization procedures with respect to the physical search are consistent with 50 U.S.C. § 1821(4)(1)-(4).[47] Under normal circumstances, these minimization procedures and any changes to them are reported to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence by the Attorney General at least 30 days before their effective date. However, if the Attorney General determines that immediate action is required, the statute mandates that he advise these committees immediately of the minimization procedures and the need for them to become effective immediately. In addition, the Attorney General must assess compliance with these minimization procedures and report such assessments to these congressional committees.

The certification of the Attorney General for a search under 50 U.S.C. § 1822 is immediately transmitted under seal to the Foreign Intelligence Surveillance Court, and maintained there under security measures established by the Chief Justice of the United States with the Attorney General's concurrence, in consultation with the Director of Central Intelligence. Such a certification remains under seal unless one of two circumstances arise: (1) either an application for a court order with respect to the physical search is made to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1821(4) (dealing with minimization procedures) and § 1823 (dealing with the process by which a federal officer, with the approval of the Attorney General, may apply for an order from the FISC approving a physical search for foreign intelligence gathering purposes); or (2) the certification is needed to determine the legality of a physical search under 50 U.S.C. § 1825 (dealing with use of the information so gathered).

In connection with physical searches under 50 U.S.C. § 1822, the Attorney General may direct a landlord, custodian or other specified person to furnish all necessary assistance needed to accomplish the physical search in a way that would both protect its secrecy and minimize interference with the services such person provides the target of the search. Such person may also be directed to maintain any records regarding the search or the aid provided under security procedures approved by the Attorney General and the Director of Central Intelligence. The provision of

---

[45](...continued)
Section 1, 60 *Fed. Reg.* 8169 (February 9, 1995), if the Attorney General makes the certifications necessary under 50 U.S.C. § 1822(a)(1).

[46]*See* 50 U.S.C. § 1801(a)(1), (2), or (3).

[47]While this is the citation cross-referenced in Section 1822, it appears that the cross-reference should read 50 U.S.C. § 1821(4)(A)-(D).

any such aid must be compensated by the Government.[48] As in the case of applications for electronic surveillance under FISA, the Foreign Intelligence Surveillance Court (FISC) has jurisdiction to hear applications and grant applications with respect to physical searches under 50 U.S.C. § 1821 *et seq.* No FISC judge may hear an application already denied by another FISC judge. If an application for an order authorizing a physical search under FISA is denied, the judge denying the application must immediately provide a written statement of reasons for the denial. If the United States so moves, the record is then transmitted under seal to the court of review established under 50 U.S.C. § 1803(b). If the court of review determines that the application was properly denied, it, in turn, must provide a written statement of the reasons for its decision, which must be transmitted under seal to the Supreme Court upon petition for certiorari by the United States.[49] Any of the proceedings with respect to an application for a physical search under FISA must be conducted expeditiously, and the record of such proceedings must be kept under appropriate security measures.

The requirements for application for an order for a physical search under FISA are included in 50 U.S.C. § 1823. While tailored to a physical search, the requirements strongly parallel those applicable to electronic surveillance under 50 U.S.C. § 1804(a)(1)-(9).[50] Like Section 1804(a)(7)(B) with respect to required

---

[48]50 U.S.C. § 1822(a)(4).

[49]50 U.S.C. § 1822(c), (d).

[50]Each application for an order approving such a physical search, having been approved by the Attorney General based upon his understanding that the application satisfies the criteria and requirements of 50 U.S.C. § 1821 *et seq.*, must be made by a Federal officer in writing upon oath or affirmation to a FISC judge. Under subsection (a) of Section 1823, the application must include:

> (1) the identity of the Federal officer making the application;
> (2) the authority conferred on the Attorney General by the President and the approval of the Attorney General to make the application;
> (3) the identity, if known, or a description of the search, and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;
> (4) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that–
>
> > (A) the target of the physical search is a foreign power or an agent of a foreign power;
> > (B) the premises or property to be searched contains foreign intelligence information; and
> > (C) the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;
>
> (5) a statement of the proposed minimization procedures;
> (6) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;
> (7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the

(continued...)

certifications for an application for electronic surveillance under FISA, Section 1823(a)(7)(B) was amended by P.L. 107-56, Section 218, to require that the Assistant to the President for National Security Affairs or designated executive branch official[51] certify, among other things, that a significant purpose (rather than "that the purpose") of the physical search is to obtain foreign intelligence information.[52] Section 1823(d) also parallels Section 1804(e) (dealing with requirements for some applications for electronic surveillance under FISA), in that, if requested in writing by the Director of

---

[50](...continued)

advice and consent of the Senate–

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the search is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);

(8) where the physical search involves a search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information; and

(9) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, premises, or property specified in the application, and the action taken on each previous application.

Under Section 1823(b), the Attorney General may require any other affidavit or certification from any other officer in connection with an application for a physical search that he deems appropriate. Under Section 1823(c), the FISC judge to whom the application is submitted may also require that the applicant provide other information as needed to make the determinations necessary under 50 U.S.C. § 1824.

[51]In Section 2 of E.O. 12949, 60 *Fed. Reg.* 8169 (February 9, 1995), the President authorized the Attorney General to approve applications to the Foreign Intelligence Surveillance Court under 50 U.S.C. § 1823, to obtain court orders for physical searches for the purpose of collecting foreign intelligence information. In Section 3 of that executive order, the President designated the Secretary of State, the Secretary of Defense, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, the Deputy Secretary of State, the Deputy Secretary of Defense, and the Deputy Director of Central Intelligence to make the certifications required by 50 U.S.C. § 1823(a)(7), in support of an application for a court order for a physical search for foreign intelligence purposes. None of these officials may exercise this authority to make the appropriate certifications unless he or she is appointed by the President, with the advice and consent of the Senate.

[52]As in the case of the change from "the purpose" to "a significant purpose" in the case of electronic surveillance, the parallel language change in Section 1823 with respect to physical searches may also have the effect of blurring the distinction between physical searches for foreign intelligence purposes and those engaged in for law enforcement purposes.

the FBI, the Secretary of Defense, the Secretary of State, or the DCI,[53] the Attorney General must personally review an application for a FISA physical search if the target is one described by Section 1801(b)(2). 50 U.S.C. § 1801(b)(2) deals with targets who knowingly engage in clandestine intelligence gathering activities involving or possibly involving violations of federal criminal laws by or on behalf of a foreign power; targets who, at the direction of an intelligence service or network of a foreign power, engage in other clandestine intelligence activities involving or potentially involving federal crimes by or on behalf of a foreign power; targets who knowingly engage in sabotage or international terrorism, activities in preparation for sabotage or international terrorism, or activities on behalf of a foreign power; targets who knowingly aid, abet, or conspire with anyone to engage in any of the previously listed categories of activities; or targets who knowingly enter the United States under false identification by or on behalf or a foreign power or who assume a false identity on behalf of a foreign power while present in the United States.[54]

Should the Attorney General, after reviewing an application, decide not to approve it, he must provide written notice of his determination to the official requesting the review of the application, setting forth any modifications needed for the Attorney General to approve it. The official so notified must supervise the making of the suggested modifications if the official deems them warranted. Unless the Attorney General or the official involved is disabled or otherwise unable to carry out his or her respective responsibilities under Section 1823, those responsibilities are non-delegable.

As in the case of the issuance of an order approving electronic surveillance under 50 U.S.C. § 1805(a), certain findings by the FISC judge are required before an order may be forthcoming authorizing a physical search for foreign intelligence information under 50 U.S.C. § 1824(a). Once an application under Section 1823 has been filed, an FISC judge must enter an ex parte order, either as requested or as modified, approving the physical search if the requisite findings are made. These include findings that:

> (1) the President has authorized the Attorney General to approve applications for physical searches for foreign intelligence purposes;
> (2) the application has been made by a Federal officer and approved by the Attorney General;
> (3) on the basis fo the facts submitted by the applicant there is probable cause to believe that–
>
> > (A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely on the basis of activities protected by the first amendment to the Constitution of the United States; and
> > (B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;

---

[53]The authority of these officials to make such a written request is non-delegable except where such official is disabled or unavailable. Each must make provision in advance for delegation of this authority should he or she become disabled or unavailable. 50 U.S.C. § 1823(d)(1)(B) and (C).

[54]See fn. 12, *supra*.

> (4) the proposed minimization procedures meet the definition of minimization contained in this subchapter; and
> (5) the application which has been filed contains all statements and certifications required by section 1823 of this title, and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1823(a)(7)(E) of this title and any other information furnished under section 1823(c) of this title.

Like Section 1805(b) regarding electronic surveillance under FISA, a FISC judge making a probable cause determination under Section 1824 may consider the target's past activities, plus facts and circumstances pertinent to the target's present or future activities.[55]

As in the case of an order under 50 U.S.C. § 1805(c) with respect to electronic surveillance, an order granting an application for a physical search under FISA must meet statutory requirements in 50 U.S.C. § 1824(c) as to specifications and directions. An order approving a physical search must specify:

> (A) the identity, if known, or a description of the target of the physical search;
> (B) the nature and location of each of the premises of property to be searched;
> (C) the type of information, material, or property to be seized, altered, or reproduced;
> (D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and
> (E) the period of time during which the physical searches are approved; . . . .

In addition, the order must direct:

> (A) that the minimization procedures be followed;
> (B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing to the target of the physical search;
> (C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the search or the aid furnished that such person wishes to retain;
> (D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and
> (E) that the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.[56]

---

[55] 50 U.S.C. § 1824(b).

[56] 50 U.S.C. § 1824(c)(1), (2).

Subsection 1824(d) sets the limits on the duration of orders under this section and makes provision for extensions of such orders if certain criteria are met.[57] Subsection 1824(e) deals with emergency orders for physical searches. It permits the Attorney General, under certain circumstances, to authorize execution of a physical search if the Attorney General or his designee informs a FISC judge that the decision to execute an emergency search has been made, and an application under 50 U.S.C. § 1821 *et seq.* is made to that judge as soon as possible, within 72 hours[58] after the Attorney General authorizes the search. The Attorney General's decision to authorize such a search must be premised upon a determination that "an emergency situation exists with respect to the execution of a physical search to obtain foreign intelligence information before an order authorizing such search can with due diligence be obtained," and "the factual basis for issuance of an order under this title [50 U.S.C.

---

[57]P.L. 107-56, Section 207(a)(2), amended 50 U.S.C. § 1824(d)(1) so that it provided:

> (1) An order under this section may approve a physical search for the period necessary to achieve its purpose, or for *90* days, whichever is less, except that *(A)* an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 101(a) [50 U.S.C. § 1801(b)(1)(A)], for the period specified in the application or for one year, whichever is less, *and (B) an order under this section for a physical search against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)] may be for the period specified in the application or for 120 days, whichever is less.*

The language in italics reflects the changes made by P.L. 107-56. The 90 day time period reflected in the first sentence replaced earlier language which provided for forty-five days.

Section 207(b)(2) of P.L. 107-56 amended 50 U.S.C. § 1824(d)(2) to provide:

> (2) Extensions of an order issued under this title [50 U.S.C. §§ 1821 et seq.] may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this Act for a physical search targeted against a foreign power, as defined in section 101(a)(5) or (6) [50 U.S.C. § 1801(a)(5) or (6)], or against a foreign power, as defined in section 101(a)(4) [50 U.S.C. § 1801(a)(4)], that is not a United States person, *or against an agent of a foreign power as defined in section 101(b)(1)(A) [50 U.S.C. § 1801(b)(1)(A)],* may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.

(Emphasis added.) Under subsection 1824(d)(3), the judge, at or before the end of the time approved for a physical search or for an extension, or at any time after the physical search is carried out, may review circumstances under which information regarding U.S. persons was acquired, retained, or disseminated to assess compliance with minimization techniques.

[58]Section 314(a)(4) of the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, amended 50 U.S.C. § 1824(e) by striking "24 hours" where it occurred and replacing it with "72 hours."

§ 1821 *et seq.*] to approve such a search exists."[59] If such an emergency search is authorized by the Attorney General, he must require that the minimization procedures required for issuance of a judicial order for a physical search under 18 U.S.C. § 1821 *et seq.* be followed.[60] If there is no judicial order for a such a physical search, then the search must terminate on the earliest of the date on which the information sought is obtained, the date on which the application for the order is denied, or the expiration of the 72 hour period from the Attorney General's authorization of the emergency search.[61] If an application for approval is denied or if the search is terminated and no order approving the search is issued, then neither information obtained from the search nor evidence derived from the search may be used in evidence or disclosed in any

> . . . trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General, if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 302 [50 U.S.C. § 1822].[62]

Subsection 1824(f) requires retention of applications made and orders granted under 50 U.S.C. § 1821 *et seq.*, for a minimum of 10 years from the date of the application.

Like 50 U.S.C. § 1806 with respect to electronic surveillance under FISA, 50 U.S.C. § 1825 restricts and regulates the uses of information secured under a FISA physical search. Such information may only be used or disclosed by Federal officers or employees for lawful purposes. Federal officers and employees must comply with minimization procedures if they use or disclose information gathered from a physical search under FISA concerning a United States person.[63] If a physical search involving the residence of a United States person is authorized and conducted under 50 U.S.C. § 1824, and at any time thereafter the Attorney General determines that there is no national security interest in continuing to maintain the search's secrecy, the Attorney General must provide notice to the United States person whose residence was searched. This notice must include both the fact that the search pursuant to FISA was conducted and the identification of any property of that person which was seized, altered, or reproduced during the search.[64] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1821 *et seq.*, must be accompanied by a

---

[59]50 U.S.C. § 1824(e)(1)(A)(i) and (ii). *See* fn.58, *supra*, regarding substitution of "72 hours" for "24 hours" in Subsection 50 U.S.C. § 1824(e)(3)(C) by P.L. 107-108, Sec. 314(a)(4).

[60]50 U.S.C. § 1824(e)(2).

[61]50 U.S.C. § 1824(e)(3).

[62]50 U.S.C. § 1824(e)(4).

[63]50 U.S.C. § 1825(a).

[64]50 U.S.C. § 1825(b).

statement that such information and any derivative information may only be used in a criminal proceeding with advance authorization from the Attorney General.[65]

The notice requirements relevant to intended use or disclosure of information gleaned from a FISA physical search or derivative information, are similar to those applicable where disclosure or use of information garnered from electronic surveillance is intended. If the United States intends to use or disclose information gathered during or derived from a FISA physical search in a trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body or other authority of the United States against an aggrieved person, the United States must first give notice to the aggrieved person, and the court or other authority.[66] Similarly, if a State or political subdivision of a state intends to use or disclose any information obtained or derived from a FISA physical search in any trial, hearing, or other proceeding before a court, department, officer, agency, regulatory body, or other State or political subdivision against an aggrieved person, the State or locality must notify the aggrieved person, the pertinent court or other authority where the information is to be used, and the Attorney General of the United States of its intention to use or disclose the information.[67] An aggrieved person may move to suppress evidence obtained or derived from a FISA physical search on one of two grounds: that the information was unlawfully acquired; or that the physical search was not made in conformity with an order of authorization or approval. Such a motion to suppress must be made before the trial, hearing or other proceeding involved unless the aggrieved person had no opportunity to make the motion or was not aware of the grounds of the motion.[68]

In camera, ex parte review by a United States district court may be triggered by receipt of notice under Subsections 1825(d) or (e) by a court or other authority; the making of a motion to suppress by an aggrieved person under Subsection 1825(f); or the making of a motion or request by an aggrieved person under any other federal or state law or rule before any federal or state court or authority to discover or obtain applications, orders, or other materials pertaining to a physical search authorized under FISA or to discover, obtain, or suppress evidence or information obtained or derived from a FISA physical search. If the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm U.S. national security, the U.S. district court receiving notice or before whom a motion or request is pending, or, if the motion is made to another authority, the U.S. district court in the same district as that authority, shall review in camera and ex parte the application, order, and such other materials relating to the physical search at issue needed to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. If the court finds it necessary to make an accurate determination of the

---

[65]50 U.S.C. § 1825(c).

[66]50 U.S.C. § 1825(d). "Aggrieved person," as defined in 50 U.S.C. § 1821(2), "means a person whose premises, property, information, or material is the target of a physical search or any other person whose premises, property, information, or material was subject to physical search."

[67]50 U.S.C. § 1825(e).

[68]50 U.S.C. § 1825(f).

legality of the search, the court may disclose portions of the application, order, or other pertinent materials to the aggrieved person under appropriate security procedures and protective orders, or may require the Attorney General to provide a summary of such materials to the aggrieved person.[69]

If the U.S. district court makes a determination that the physical search was not lawfully authorized or conducted, then it must "suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person." If, on the other hand, the court finds that the physical search was lawfully authorized or conducted, the motion of the aggrieved person will be denied except to the extent that due process requires discovery or disclosure.[70]

If the U.S. district court grants a motion to suppress under 50 U.S.C. § 1825(h); deems a FISA physical search unlawfully authorized or conducted; or orders review or grants disclosure of applications, orders or other materials pertinent to a FISA physical search, that court order is final and binding on all federal and state courts except a U.S. Court of Appeals or the U.S. Supreme Court.[71]

As a general matter, where an emergency physical search is authorized under 50 U.S.C. § 1824(d), and a subsequent order approving the resulting search is not obtained, any U.S. person named in the application and any other U.S. persons subject to the search that the FISC judge deems appropriate in the interests of justice must be served with notice of the fact of the application and the period of the search, and must be advised as to whether information was or was not obtained during that period.[72] However, such notice may be postponed or suspended for a period not to exceed 90 days upon an ex parte showing of good cause to the judge, and, upon further good cause shown, the court must forego such notice altogether.[73]

Section 504(b) of P.L. 107-56, added a new 50 U.S.C. § 1825(k) to the statute, which deals with consultation by federal officers doing FISA searches with federal law enforcement officers. Under this new language, federal officers "who conduct physical searches to acquire foreign intelligence information" under 50 U.S.C. § 1821 *et seq.*, may consult with federal law enforcement officers:

> . . . to coordinate efforts to investigate or protect against
> (A)actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

---

[69]50 U.S.C. § 1825(g).

[70]50 U.S.C. § 1825(h).

[71]50 U.S.C. § 1825(i).

[72]50 U.S.C. § 1825(j)(1).

[73]50 U.S.C. § 1825(j)(2).

> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.[74]

Such coordination does not preclude certification required under 50 U.S.C. § 1823(a)(7) or entry of an order under 50 U.S.C. § 1824.[75]

50 U.S.C. § 1826 provides for semiannual congressional oversight of physical searches under FISA. The Attorney General is directed to "fully inform" the permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate with respect to all physical searches conducted under 50 U.S.C. § 1821 *et seq.* Also on a semiannual basis, the Attorney General is required to provide a report to those committees and to the House and Senate Judiciary Committees setting forth: the total number of applications for orders approving FISA physical searches during the preceding 6 month period; the total number of those orders granted, modified, or denied; the number of such physical searches involving the residences, offices, or personal property of United States persons; and the number of occasions, if any, the Attorney General gave notice under 50 U.S.C. § 1825(b).[76]

Section 1827 imposes criminal sanctions for intentionally executing a physical search for foreign intelligence gathering purposes under color of law within the United States except as authorized by statute. In addition, criminal penalties attach to a conviction for intentionally disclosing or using information obtained by a physical search under color of law within the United States for the purpose of gathering intelligence information, where the offender knows or has reason to know that the information was obtained by a physical search not authorized by statute. In either case, this section provides that a person convicted of such an offense faces a fine of not more than $10,000,[77] imprisonment for not more than 5 years or both. Federal jurisdiction attaches where the offense is committed by an officer or employee of the United States. It is a defense to such a prosecution if the defendant was a law enforcement or investigative officer engaged in official duties and the physical search was authorized and conducted pursuant to a search warrant or court order by a court of competent jurisdiction.

In addition, an aggrieved person other than a foreign power or an agent of a foreign power as defined under section 1801(a) or 1801(b)(1)(A),[78] whose premises, property, information, or material within the United States was physically searched under FISA; or about whom information obtained by such a search was disclosed or used in violation of 50 U.S.C. § 1827, may bring a civil action for actual damages,

---

[74]50 U.S.C. § 1825(k)(1).

[75]50 U.S.C. § 1825(k)(2).

[76]*See* fn. 64, *supra*, and accompanying text.

[77]This section was added in 1994 as Title III, Section 307 of P.L. 95-511, by P.L. 103-359, Title VIII, § 807(a)(3), 108 Stat. 3452. If a fine were to be imposed under the general fine provisions 18 U.S.C. § 3571, rather than under the offense provision, the maximum fine would be $250,000 for an individual.

[78]For definitions, *see* fn. 14, *supra.*

punitive damages, and reasonable attorney's fees and other investigative and litigation costs reasonably incurred.[79]

In times of war, the President, through the Attorney General, may authorize physical searches under FISA without a court order to obtain foreign intelligence information for up to 15 days following a declaration of war by Congress.[80]

Pen registers or trap and trace devices[81] used for foreign intelligence gathering purposes. Title IV of FISA, 50 U.S.C. § 1841 *et seq.*, was added in 1998, significantly amended by P.L. 107-56,[82] and amended further by Section 314(5) of P.L. 107-108. Under 50 U.S.C. § 1842(a)(1), notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may apply for an order or extension of an order authorizing or approving the installation and use of a pen register or trap and trace device "*for any investigation to protect against international terrorism or clandestine intelligence activities, provided such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution*" conducted by the Federal Bureau of Investigation (FBI) under guidelines approved by the Attorney General pursuant to E.O. 12333 or a successor order.[83] This authority is separate from the authority to conduct electronic surveillance under 50 U.S.C. § 1801 *et seq.*[84]

---

[79]50 U.S.C. § 1828. Actual damages are defined to be "not less than liquidated damages of $1,000 or $100 per day for each violation, whichever is greater." 50 U.S.C. § 1828(1).

[80]50 U.S.C. § 1829.

[81]Under 50 U.S.C. § 1841(2), the terms "pen register" and "trap and trace device" are given the meanings in 18 U.S.C. § 3127. Under Section 3127, "pen register"

> . . . means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; . . . .

As defined by 18 U.S.C. § 3127(4), "trap and trace device" "means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 50 U.S.C. § 1841 is the section that defines terms applicable to the pen register and trap and trace device portions of FISA.

[82]Title IV of FISA was added by Title VI, Sec. 601(2) of P.L. 105-272, on October 20, 1998, 112 Stat. 2405-2410., and amended by P.L. 107-56 and by P.L. 107-108.

[83]The italicized language was added by P.L. 107-56, Section 214(a)(1), replacing language which had read "for any investigation to gather foreign intelligence information or information concerning international terrorism."

[84]50 U.S.C. § 1842(a)(2).

Each such application is made in writing upon oath or affirmation to a FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant orders approving installation of pen registers or trap and trace devices on behalf of a FISC judge. The application must be approved by the Attorney General or a designated attorney for the Government. Each application must identify the federal officer seeking to use the pen register or trap and trace device sought in the application. It must also include a certification by the applicant "*that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.*"[85]

Under 50 U.S.C. § 1842, as amended by P.L. 107-56, pen registers and trap and trace devices may now be installed and used not only to track telephone calls, but also other forms of electronic communication such as e-mail. Once an application is made under Section 1842, the judge[86] must enter an ex parte order[87] as requested or as

---

[85]This language, added by P.L. 107-56, Section 214(a)(2), replaced stricken language which read:

> (2) a certification by the applicant that the information to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General; and
> (3) information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with--
> (A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or
> (B) a foreign power or agent of a foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

[86]This section refers simply to "judge." In light of 50 U.S.C. § 1842(b), it would appear that this may refer to either a FISC judge or a U.S. magistrate judge designated by the Chief Justice under Section 1842(b)(2) to hear applications for and grant orders approving installation and use of pen registers or trap and trace devices on behalf of a FISC judge. The legislative history on this provision does not appear to clarify this point. The language was included in the bill reported out as an original measure by the Senate Select Committee on Intelligence, S. 2052, as Sec. 601. The Committee's report, S. Rept. 105-185, indicates that magistrate judges were included in the legislation to parallel their use in connection with receipt of applications and approval of pen registers and trap and trace devices in the context of criminal investigations, but reflected the Committee's understanding that the authority provided in the legislation to designate magistrate judges to consider applications for pen registers and trap and trace devices in the foreign intelligence gathering context would be closely monitored by the Department of Justice and this designation authority would not be exercised until the Committee was briefed on the compelling need for such designations,

(continued...)

[86](...continued)
as reflected, for example, through statistical information on the frequency of applications to the FISC under the new procedure. S. Rept. 105-185, at 28 (May 7, 1998). The provision creating on pen registers and trap and trace devices in foreign intelligence and international terrorism investigations, Sec. 601 of the bill as passed, was among those included in the conference version of H.R. 3694 which was passed in lieu of S. 2052. H. Conference Rept. 105-80, at 32 (October 5, 1998).

[87]Under 50 U.S.C. § 1842(d)(2)(A), such an order

> *(A) shall specify--*
> *(i) the identity, if known, of the person who is the subject of the investigation;*
> *(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;*
> *(iii) the attributes of the communications to which the order applies, such as the number or other identifies, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.*
> (B) shall direct that–
> (i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;
> (ii) such provider, landlord, custodian, or other person–
> (I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and
> (II) shall maintain, under security procedures approved by the Attorney General and the Director of Central Intelligence pursuant to section 1805(b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; and
> (iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance.

The italicized portions of this section reflect amended language from P.L. 107-56, Section 214 (a)(4).

P.L. 107-108, Section 314(a)(5)(B), replaced "of a court" at the end of 50 U.S.C. § 1842(f) with "of an order issued," so that the language now reads:

> (f) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance

(continued...)

modified approving the installation and use of a pen register or trap and trace device if the application meets the requirements of that section.

Section 1843 of Title 18 of the United States Code focuses upon authorization for installation and use of a pen register or trap and trace device under FISA during specified types of emergencies. This provision applies when the Attorney General makes a reasonable determination that:

> (1) an emergency requires the installation and use of a pen register or trap and trace device to obtain *foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of a activities protected by the first amendment to the Constitution* before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and
> (2) the factual basis for issuance of an order under section 1842(c) of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.[88]

Upon making such a determination, the Attorney General may authorize the installation and use of a pen register or trap and trace device for this purpose if two criteria are met. First, the Attorney General or his designee must inform a judge referred to in Section 1842(b)[89] at the time of the emergency authorization that the decision to install and use the pen register or trap and trace device has been made. Second, an application for a court order authorizing a pen register or trap and trace device under 50 U.S.C. § 1842(a)(1) must be made to the judge as soon as practicable, but no later that 48 hours after the emergency authorization.[90] If no order approving the installation and use of a pen register or trap and trace device is forthcoming, then the installation and use of such pen register or trap and trace device must terminate at the earlier of the time when the information sought is obtained, the time when the application for the order is denied under 50 U.S.C. § 1842, or the

---

[87](...continued)
with the terms *of an order issued* under this section.

(Emphasis added.) *Cf.*, 50 U.S.C. § 1805(f), which contains an immunity grant which, at first blush would appear to apply only to electronic surveillance under FISA, but which has been interpreted in H. Rept. 107-328, page 25, the conference committee accompanying H.R. 2883, which became P.L. 107-108, to apply to electronic surveillance, physical searches and pen register and trap and trace devices. See discussion at fn. 32, *supra.*

[88]50 U.S.C. § 1843(b) (italics reflect language added by P.L. 107-56, § 214(b)(2), in place of language which read "foreign intelligence information or information concerning international terrorism.") Similar language was inserted in 50 U.S.C. § 1843(a) by P.L. 107-56, § 214(b)(1), in place of language that paralleled that stricken from subsection 1843(b).

[89]See discussion of the term "judge" as used in Section 1842(b) in fn. 86, *supra.*

[90]50 U.S.C. § 1843(a).

expiration of 48 hours from the time the Attorney General made his emergency authorization.[91]

If an application for an order sought under Section 1843(a)(2) is denied, or if the installation and use of the pen register or trap and trace device is terminated, and no order approving it is issued under 50 U.S.C. § 1842(b)(2), then no information obtained or evidence derived from the use of the pen register or trap and trace device may be received in evidence or disclosed in any trial, hearing or other proceeding in any court, grand jury, department, office, agency, regulatory body, legislative committee or other federal state or local authority. Furthermore, in such circumstances, no information concerning a United States person acquired from the use of the pen register or trap and trace device may later be used or disclosed in any other way by federal officers or employees without consent of the U.S. person involved, with one exception. If the Attorney General approves the disclosure because the information indicates a threat of death or serious bodily harm to anyone, then disclosure without consent of the U.S. person involved is permitted.[92]

If Congress declares war, then, notwithstanding any other provision of law, the President, through the Attorney General, may authorize use of a pen register or trap and trace device without a court order to acquire foreign intelligence information for up to 15 calendar days after the declaration of war.[93]

50 U.S.C. § 1845 sets parameters with respect to the use of information obtained through the use of a pen register or trap and trace device under 50 U.S.C. § 1841 *et seq.* Federal officers and employees may only use or disclose such information with respect to a U.S. person without the consent of that person in accordance with Section 1845.[94] Any disclosure by a Federal officer or employee of information acquired pursuant to FISA from a pen register or trap and trace device must be for a lawful purpose. [95] Disclosure for law enforcement purposes of information acquired under 50 U.S.C. § 1841 *et seq.* is only permitted where the disclosure is accompanied by a statement that the information and any derivative information may only be used in a criminal proceeding with the advance authorization of the Attorney General.[96]

Under 50 U.S.C. § 1845(c), when the United States intends to enter into evidence, use, or disclose information obtained by or derived from a FISA pen register or trap and trace device against an aggrieved person[97] in any federal trial,

---

[91]50 U.S.C. § 1843(c)(1).

[92]50 U.S.C. § 1843(c)(2).

[93]50 U.S.C. § 1844.

[94]50 U.S.C. § 1845(a)(1).

[95]50 U.S.C. § 1845(a)(2).

[96]50 U.S.C. § 1845(b).

[97]"Aggrieved person" is defined in 50 U.S.C. § 1841(3) for purposes of 50 U.S.C. § 1841 *et seq.* as any person:

(continued...)

hearing, or proceeding, notice requirements must be satisfied. The Government, before the trial, hearing, or proceeding or a reasonable time before the information is to be proffered, used or disclosed, must give notice of its intent both to the aggrieved person involved[98] and to the court or other authority in which the information is to be disclosed or used.

If a state or local government intends to enter into evidence, use, or disclose information obtained or derived from such a trap and trace device against an aggrieved person in a state or local trial, hearing or proceeding, it must give notice to the aggrieved person and to the Attorney General of the United States of the state or local government's intent to disclose or use the information.[99]

The aggrieved person in either case may move to suppress the evidence obtained or derived from a FISA pen register or trap and trace device on one of two grounds: that the information was unlawfully acquired; or that the use of the pen register or trap and trace device was not made in conformity with an order of authorization or approval under 50 U.S.C. 1841 *et seq.*[100]

If notice is given under 50 U.S.C. §§ 1845(c) or (d), or a motion or request is made to suppress or to discover or obtain any applications, orders, or other materials relating to use of a FISA pen register or trap and trace device or information obtained by or derived from such use, the Attorney General may have national security concerns with respect to the effect of such disclosure or of an adversary hearing. If he files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, the United States district court in which the motion or request is made, or where the motion or request is made before another authority, the U.S. district court in the same district, shall review *in camera* and *ex parte* the application, order, and other relevant materials to determine whether the use of the pen register or trap and trace device was lawfully authorized and conducted.[101] In so doing, the court may only disclose portions of the application, order or materials to the aggrieved person or order the Attorney General to provide the aggrieved person with a summary of these materials if that disclosure is necessary to making an

---

[97](...continued)

(A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by subchapter IV [50 U.S.C. § 1841 et seq.]; or

(B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by subchapter IV to capture incoming electronic or other communications impulses.

[98]The statute refers to notice to the "aggrieved person." Here it is using this term in the context of a pen register or trap and trace device, as defined in 50 U.S.C. § 1841(3) (see fn. 97, *supra).* This term is also defined in both 50 U.S.C. §§ 1801(k) (in the context of electronic surveillance, see fn. 35, *supra*) and 1825(d) (in the context of a physical search, see fn. 66, *supra*).

[99]50 U.S.C. § 1845(d).

[100]50 U.S.C. § 1845(e).

[101]50 U.S.C. § 1845(f)(1).

accurate determination of the legality of the use of the pen register or trap and trace device.[102]

Should the court find that the pen register or trap and trace device was not lawfully authorized or conducted, it may suppress the unlawfully obtained or derived evidence or "otherwise grant the motion of the aggrieved person."[103] On the other hand, if the court finds the pen register or trap and trace device lawfully authorized and conducted, it may deny the aggrieved person's motion except to the extent discovery or disclosure is required by due process.[104] Any U.S. district court orders granting motions or request under Section 1845(g), finding unlawfully authorized or conducted the use of a pen register or trap and trace device, or requiring review or granting disclosure of applications, orders or other materials regarding installation and use of a pen register or trap and trace device are deemed final orders. They are binding on all federal and state courts except U.S. courts of appeals and the U.S. Supreme Court.[105]

Section 1846 deals with congressional oversight of the use of FISA pen registers and trap and trace devices. It requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence regarding all FISA uses of pen registers and trap and trace devices. In addition, the Attorney General, on a semi-annual basis, must report to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, the House Judiciary Committee and the Senate Judiciary Committee on the total number of applications made for orders approving the use of such pen registers and trap and trace devices and the total number of such orders granted, modified, or denied during the previous 6 month period.

Access to certain business records for foreign intelligence purposes. Also added in 1998, Title V of FISA, 50 U.S.C. § 1861 *et seq.*, was substantially changed by P.L. 107-56 and modified further by P.L. 107-108.[106]

---

[102]50 U.S.C. § 1845(f)(2).

[103]50 U.S.C. § 1845(g)(1).

[104]50 U.S.C. § 1845(g)(2).

[105]50 U.S.C. § 1845(h).

[106]Title V of FISA was added by Title VI, Sec. 602, of P.L. 105-272, on October 20, 1998, 112 Stat. 2411-12, and significantly amended by P.L. 107-56 and P.L. 107-108. The prior version of 50 U.S.C. § 1861 provided definitions for "foreign power," "agent of a foreign power," "foreign intelligence information," "international terrorism," and "Attorney General," "common carrier," "physical storage facility," "public accommodation facility," and "vehicle rental facility" for purposes of 50 U.S.C. § 1861 *et seq.* The prior version of Section 1862 was much more narrowly drawn than the new version added in P.L. 107-56 and amended by P.L. 107-108. The earlier version read:

> (a) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order authorizing a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to

(continued...)

Although denominated "access to certain business records for foreign intelligence and international terrorism investigations," the reach of Section 1861, as amended by the

---

[106](...continued)

release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism which investigation is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(b) Each application under this section–

(1) shall be made to–

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28 [28 U.S.C. § 631 *et seq.*], who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the release of records under this section on behalf of a judge of that court; and

(2) shall specify that–

(A) the records concerned are sought for an investigation described in subsection (a); and

(B) there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.

(c)(1) Upon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application satisfied the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d)(1) Any common carrier, public accommodation facility, physical storage facility, or vehicle rental facility shall comply with an order under subsection (c).

(2) No common carrier, public accommodation facility, physical storage facility, or vehicle rental facility, or officer, employee, or agent thereof, shall disclose to any person (other than those officers, agents, or employees of such common carrier, public accommodation facility, physical storage facility, or vehicle rental facility necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section) that the Federal Bureau of Investigation has sought or obtained records pursuant to an order under this section.

Congressional oversight was covered under the prior provisions by 50 U.S.C. §1863, which was similar, but not identical to the new Section 1862. The former Section 1863 stated:

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all request for records under this subchapter [50 U.S.C. § 1861 *et seq.*].

(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period–

(1) the total number of applications made for orders approving requests for records under this subchapter [50 U.S.C. § 1861 *et seq.*]; and

(2) the total number of such orders either granted, modified, or denied.

USA PATRIOT Act and P.L. 107-108, is now substantially broader than business records alone. Under 50 U.S.C. § 1861(a)(1), the Director of the FBI, or his designee (who must be at the Assistant Special Agent in Charge level or higher in rank) may apply for an order requiring

> . . . the production of any tangible things (including books, records, papers, documents, and other items) for an investigation *to obtain foreign intelligence information not concerning a United States person or* to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[107]

Subsection 1861(a)(2) requires that such an investigation must be conducted under guidelines approved by the Attorney General under E.O. 12333 or a successor order and prohibits such an investigation of a United States person based solely upon First Amendment protected activities.

An application for an order under Section 1861 must be made to an FISC judge or to a U.S. magistrate judge publicly designated by the Chief Justice of the United States to hear such applications and grant such orders for the production of tangible things on behalf of an FISC judge.[108] The application must specify that the "records"[109] are sought for "an authorized investigation conducted in accordance with

---

[107]The italicized portion of Section 1861(a)(1) was added by Section 314(a)(6) of P.L. 107-108. H. Rept. 107-328, the conference report to accompany H.R. 2883, the Intelligence Authorization Act for Fiscal Year 2002 (which became P.L. 107-108), at page 24, describes the purpose of this addition as follows:

> Section 215 of the USA PATRIOT Act of 2001 amended title V of the FISA, adding a new section 501 [50 U.S.C. § 1861]. Section 501(a) now authorizes the director of the FBI to apply for a court order to produce certain records "For an investigation to protect against international terrorism or clandestine intelligence activities." Section 501(b)(2) directs that the application for such records specify that the purpose of the investigation is to "obtain foreign intelligence information not concerning a United States person." However, section 501(a)(1), which generally authorizes the applications, does not contain equivalent language. Thus, subsections (a)(1) and (b)(2) now appear inconsistent.
>
> The conferees agreed to a provision which adds the phrase "to obtain foreign intelligence information not concerning a United States person or" to section 501(a)(1). This would make the language of section 501(a)(1) consistent with the legislative history of section 215 of the USA PATRIOT Act (*see* 147 Cong. Res. S11006 (daily ed. Oct. 25, 2001) (sectional analysis)) and with the language of section 214 of the USA PATRIOT Act (authorizing an application for an order to use pen registers and trap and trace devices to "obtain foreign intelligence information not concerning a United States person.").

[108]50 U.S.C. § 1861(b)(1).

[109]While the language refers to "records," it is worthy of note that the authority conferred upon the Director of the FBI or his designee under Section 1861(a) encompasses applications for orders requiring production of "any tangible thing (including books, (continued...)

[50 U.S.C. § 1862(a)(2)] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[110] When such an application is made, the judge must enter an *ex parte* order "as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section."[111] Such an order shall not disclose that it is issued for purposes of an investigation under 50 U.S.C. § 1861(a).[112] Subsection 1861(d) prohibits any person to disclose that the FBI has sought or obtained tangible things under Section 1861, except where the disclosure is made to persons necessary to the production of tangible things involved. Subsection 1861(e) precludes liability for persons who, in good faith, produce tangible things under such a Section 1861 order. It further indicates that production does not constitute a waiver of any privilege in any other proceeding or context.

50 U.S.C. § 1862 deals with congressional oversight. Subsection 1862(a) requires the Attorney General semiannually to fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence regarding all request for production of tangible things under Section 1861.[113] Subsection 1862(b) requires the Attorney General to report to the House and Senate Judiciary Committees on the total number of applications for Section 1861 orders for production of tangible things and on the total number of such orders granted, modified, or denied during the previous 6 months.

New Private Right of Action

In addition to provisions which amended FISA explicitly, other provisions of the USA PATRIOT Act touched upon FISA, at least tangentially. For example, Section 223 of the Act, among other things, created a new 18 U.S.C. § 2712. This new section, in part, created an exclusive private right of action for any person aggrieved by any willful violation of sections 106(a), 305(a), or 405(a) of FISA (50 U.S.C. §§ 1806(a), 1825(a), 1845(a), respectively) to be brought against the United States in U.S. district court to recover money damages. Such monetary relief would amount

---

[109](...continued)
records, papers, documents, and other items)." One might argue, therefore, that for Subsection 1861(a)(1) and Subsection 1861(b)(2) to be read in harmony, a court might interpret "records" more broadly to cover "any tangible thing." On the other hand, if, by virtue of the specific reference in Subsection 1861(a)(1) to "records" as only one of many types of "tangible things,"the term "records" in Subsection 1861(b)(2) were to be read narrowly, it might lead to some confusion as to the nature and scope of any specification that might be required where an application seeking production of types of tangible things other than records is involved.

[110]50 U.S.C. § 1861(b)(2).

[111]50 U.S.C. § 1861(c)(1).

[112]50 U.S.C. § 1861(c)(2).

[113]Section 314(a)(7) of P.L. 107-108 corrected two references in 50 U.S.C. § 1862 as passed in the USA PATRIOT Act. P.L. 107-108 replaced "section 1842 of this title" with "section 1861 of this title," in both places in 50 U.S.C. § 1862 where it appeared.

to either actual damages or $10,000, whichever is greater; and reasonably incurred litigation costs. It also set forth applicable procedures.[114]

USA PATRIOT Act Sunset Provision

Section 224 of the USA PATRIOT Act set a sunset for many of the provisions in the Act of December 31, 2005. Among those provisions which will sunset pursuant to this are all of the amendments to FISA, and subsequent amendments thereto, except the provision which increased the number of FISC judges from 7 to 11 (Section 208 of P.L. 107-56). Section 224 also excepts from the application of the sunset provision any particular foreign intelligence investigations that began before December 31, 2005, or any particular offenses or potential offenses which began or occurred before December 31, 2005. As to those particular investigations or offenses, applicable provisions would continue in effect.

Conclusion

The Foreign Intelligence Surveillance Act, as amended, provides a statutory structure to be followed where electronic surveillance, 50 U.S.C. § 1801 *et seq.*, physical searches, 50 U.S.C. § 1821 *et seq.*, or pen registers or trap and trace devices, 50 U.S.C. § 1841 *et seq.*, for foreign intelligence gathering purposes are contemplated. It creates enhanced procedural protections where a United States person is involved, while setting somewhat less stringent standards where the surveillance involves foreign powers or agents of foreign powers. With its detailed statutory structure, it appears intended to protect personal liberties safeguarded by the First and Fourth Amendments while providing a means to ensure national security interests.

The USA PATRIOT Act, P.L. 107-56, increased the number of FISC judges from 7 to 11, while expanding the availability of FISA electronic surveillance, physical searches and pen registers and trap and trace devices. For example, under P.L. 107-56, an application for a court order permitting electronic surveillance or a physical search under FISA is now permissible where "a significant" purpose of the surveillance or physical search, rather than "the" purpose or, as interpreted by some courts, the primary purpose of the surveillance is to gather foreign intelligence information. While the previous language withstood constitutional challenge, the

---

[114]Another provision, Section 901 of the USA PATRIOT Act, amended 50 U.S.C. § 403-3(c) (Section 103(c) of the National Security Act of 1947) regarding the responsibilities of the Director of Central Intelligence (DCI). The amendment added to those authorities and responsibilities, placing upon the DCI the responsibility for the establishment of

> . . . requirements and priorities for foreign intelligence information to be collected under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.), and provide assistance to the Attorney General to ensure that information derived from electronic surveillance or physical searches under that Act is disseminated so it may be used efficiently and effectively for foreign intelligence purposes, except that the Director shall have no authority to direct, manage, or undertake electronic surveillance or physical search operations pursuant to that Act unless otherwise authorized by statute or Executive order.

constitutional sufficiency of the change in the FISA procedures under the Fourth Amendment is, as yet, untested.

The USA PATRIOT Act also amended FISA to allow court orders permitting so-called multipoint or "roving" electronic surveillance, where the orders do not require particularity with respect to the identification of the instrument, place, or facility to be intercepted, upon a finding by the court that the actions of the target of the surveillance are likely to thwart such identification. P.L. 107-108 further clarified this authority.

Under the Act, pen registers and trap and trace devices may now be authorized for e-mails as well as telephone conversations. In addition, the Act expanded the previous FBI access to business records, permitting court ordered access in connection with a foreign intelligence or international terrorism investigation not just to business records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities, but to any tangible things.

While expanding the authorities available for foreign intelligence investigations, FISA, as amended by the USA PATRIOT Act and the Intelligence Authorization Act for FY 2002, also contains broader protections for those who may be the target of the various investigative techniques involved. For example, whether the circumstances involve electronic surveillance, physical searches, pen registers or trap and trace devices or access to business records and other tangible items, FISA, as amended by the USA PATRIOT Act, does not permit the court to grant orders based solely upon a United States person's exercise of First Amendment rights.[115]

In addition, P.L. 107-56 created a new private right of action for persons aggrieved by inappropriate disclosure or use of information gleaned or derived from electronic surveillance, physical searches or the use of pen registers or trap and trace devices. These claims can be brought against the United States for certain willful violations by government personnel.

Finally, the inclusion of a sunset provision for the FISA changes made in the USA PATRIOT Act, with the exception of the increase in the number of FISC judges, provides an opportunity for the new authorities to be utilized and considered, and an opportunity for the Congress to revisit them in light of that experience.

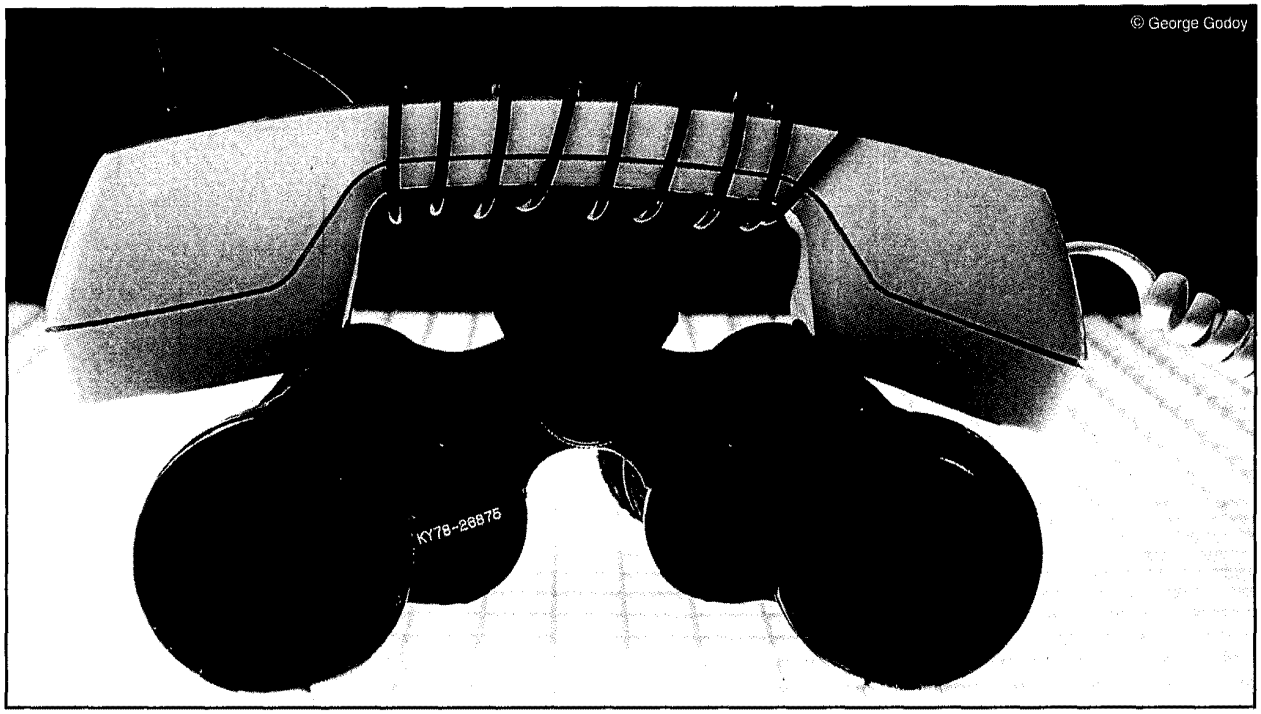
---

[115] *See, e.g.*, 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A), 1842(a)(1), 1843(b), 1861(a)(1), and 1861(a)(2).

Foreign Intelligence Surveillance Act

Before and After the USA PATRIOT Act

By MICHAEL J. BULZOMI, J.D.



The terrorist attacks of September 11, 2001, left an indelible mark upon America and an overshadowing feeling of vulnerability. They also created a determination to respond to the new national security threats they represented. Congress reacted to these threats by passing laws providing new tools to fight terrorism. Perhaps, the most controversial recent act of Congress is the United and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001[1] (USA PATRIOT Act) and its impact upon the use of electronic surveillance and physical searches authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA)[2] to combat foreign threats.

Some Americans fear the actions taken by Congress may infringe upon basic American liberties. Benjamin Franklin warned that " those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety."[3] The government must use its new tools in a way that preserves the rights and freedoms guaranteed by America's democracy, but, at the same time, ensure that the fight against terrorism is vigorous and effective. No American should be forced to seek safety over liberty. This article briefly examines FISA and the impact of the USA PATRIOT Act upon it.

FISA

Electronic monitoring (including both wiretaps and microphone installations) and physical searches

are excellent, and sometimes essential, sources of information for both foreign intelligence and criminal activities. In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act. Title III of that act[4] contains provisions concerning the authorization and use of electronic monitoring by the government to gather information regarding criminal activities. Under Title III, the government has specific authorization procedures and rules to follow when it monitors people and places to collect evidence of violations of criminal laws. But, Title III did not answer the question of whether or not the government is required to obtain court authorization for electronic monitoring conducted, not for criminal investigations but for the collection of information regarding threats to national security.

The U.S. Supreme Court faced this issue in the case of *United States v. United States District Court.*[5] In this case, a group of Vietnam War protesters tried to blow up the local CIA recruiting office in Ann Arbor, Michigan, and a number of other government buildings. Evidence obtained during a domestic national security wire interception, undertaken without a formal court order, was used in the subsequent criminal trial. The use of this evidence was contested. The issue was whether or not the president had the authority, through the attorney general, to authorize electronic surveillance for national security matters without prior judicial review. The Court held that the government does not have unlimited power to conduct national security wiretaps for domestic security matters, and that prior judicial authorization is needed before using wiretaps for national security purposes. However, the Court recognized that such wiretaps involve different policy and practical considerations from ordinary criminal wiretaps. It suggested that Congress consider exploring the issue and decide if the authorization for and rules governing the use of national security wiretaps should be the same as those governing criminal wiretaps. The Court made it clear that it was not deciding the issue of the government's authority to conduct wiretaps in cases of foreign threats to the national security.

To establish the necessary authority and procedures for the government to conduct wiretaps in response to foreign threats, Congress passed FISA. FISA established a requirement of judicial approval before the government engages in an electronic surveillance (as well as physical searches) for foreign intelligence purposes. The act established the FISA Court, consisting of U.S. District Court judges designated by the chief justice of the U.S. Supreme Court. The court's purpose is to review government applications for national security electronic monitoring and searches and authorize their use with appropriate limitations. If the FISA Court denies an application for an order authorizing a national security wiretap or search, the matter is referred under seal to the FISA Court of Review, comprised of three federal judges selected by the chief justice of the U.S. Supreme Court. The court of review determines whether the application was properly denied.[6] Its decision can be appealed directly to the U.S. Supreme Court.

Special Agent Bulzomi is a legal instructor at the FBI Academy.

"The government must use its new tools in a way that preserves the rights and freedoms guaranteed by America's democracy, but, at the same time, ensure that the fight against terrorism is vigorous and effective."

FISA Contrasted with Title III

In essence, the purpose of a FISA order is to gather foreign intelligence information,[7] while the purpose of a Title III wiretap order is to gather evidence for criminal prosecution. The FISA application

need only state facts supporting probable cause to believe that the target of the intercept (or search) is a foreign power, or an agent of a foreign power, and that the facilities to be monitored or searched are being used, or are about to be used, by a foreign power, or an agent of a foreign power, and to certify that a significant purpose of the surveillance is to obtain foreign intelligence information.[8] To show that a person is an agent of a foreign power, the government need only relate facts demonstrating that the subject is an officer or employee of a foreign power or acts on the foreign power's behalf; or knowingly engages in clandestine intelligence-gathering activities that may involve a violation of U.S. criminal statutes; or knowingly engages in sabotage, international terrorism, or in the preparation of these activities on behalf of a foreign power.[9]

In contrast, a criminal Title III wiretap must be supported by probable cause to believe that a specific individual, using an identified phone or location, is committing a particular crime.[10] It requires that the government show that a predicate offense is, has, or will be committed by the subject of the surveillance[11] and that particular communications concerning the predicate offense will be obtained through the wiretap[12] at a specified location or through a specified device used by the target.[13]

FISA Information for Criminal Prosecutions

It is important to note that both FISA and Title III require a showing of probable cause to authorize electronic monitoring (and physical searches in the case of FISA). However, because of the differing objectives of the two acts, the degree of specificity required differs markedly. Arguably, because of the different probable cause showing required by FISA, it is easier for the government to obtain a FISA order than it is to obtain a Title III order. Because of this, the courts became concerned that the government

> ***"...both FISA and Title III require a showing of probable cause to authorize electronic monitoring (and physical searches in the case of FISA)."***

would obtain FISA electronic surveillance orders in what were essentially criminal investigations to avoid the stricter requirements of Title III.

This concern surfaced in an espionage case that predates FISA. In *United States v. Truong Dinh Hung,*[14] the government used a warrantless wiretap to overhear and record telephone conversations of the defendant and to bug his apartment. The wiretapping and bugging were authorized by the attorney general under the "foreign intelligence" exception to the Fourth Amendment. The defendant moved to suppress the evidence collected by means of the wiretap and bug as violations of the Fourth Amendment. The U.S. Court of Appeals for the Fourth Circuit admitted the evidence collected during the early days of the collection but held that evidence obtained after the primary purpose of the investigation had shifted from securing intelligence information to accumulating evidence of a crime and must be suppressed because of the failure to comply with the requirements of Title III. This ruling is the origin of the "primary purpose" test that was to create problems in later cases.

Subsequent cases decided after the passage of FISA distinguished *Truong* on the grounds that the surveillance authorization in that case was not obtained pursuant to a FISA warrant.[15] These courts noted that FISA contains a statutory mechanism for the dissemination of criminal information obtained during an intelligence intercept and have held that when such evidence is discovered "incidentally" during an authorized FISA intercept it may be admitted in subsequent criminal prosecutions.[16] This would include situations where "the government can anticipate that the fruits of such surveillance may later be used, as allowed by [the statute], as evidence in a criminal trial."[17] This line of reasoning became known as the "primary purpose" test and was adopted by several circuits.[18] In other words, when the primary object of the electronic monitoring (or search) was to collect foreign intelligence information, FISA was the appropriate mechanism to seek authorization from the courts. When the primary purpose was to seek criminal prosecution, Title III was the appropriate mechanism. Failure

to strictly observe this distinction resulted in a possible suppression of the evidence.

The "primary purpose" test led the FISA Court and the U.S. Department of Justice (DOJ) to adopt a policy of building a "wall" between intelligence investigators and criminal investigators for fear of tainting FISA court ordered surveillances. Intelligence investigators were not to discuss ongoing foreign intelligence or foreign counterintelligence investigations with criminal investigators. In this way, FISA orders could not be used by criminal investigators to avoid seeking Title III orders. This practice led to a critical lack of coordination in investigations, such as international terrorism cases, which have both intelligence and criminal aspects.

FISA AS AMENDED BY THE USA PATRIOT ACT

Following the September 11, 2001, terrorist attacks, Congress reassessed intelligence-gathering procedures and passed the USA PATRIOT Act. The most significant changes involve the purposes for which FISA-authorized electronic monitoring and searches may be used and the exchange of information between criminal and foreign intelligence investigators.

Previously, FISA-authorized electronic monitoring and searches only could be used if high-level executive officials certified that "the purpose" was to obtain foreign intelligence information. As noted, that language came to be interpreted as the "primary purpose" by the courts and DOJ. The USA PATROIT Act now requires that foreign intelligence information gathering be a "significant purpose."[19] The act amends FISA so that intelligence officials may coordinate efforts with law enforcement officials to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities without undermining the required certification of the "significant purpose" of FISA orders. The result is that Congress rejected the idea of having a "wall" between foreign intelligence and law enforcement officials when the object of the investigation is to detect, prevent, or prosecute foreign intelligence crimes.

On March 6, 2002, Attorney General John D. Ashcroft implemented the USA PATRIOT Act by establishing a new DOJ policy regarding information-sharing procedures. The new procedures permitted the complete exchange of information and advice between intelligence officers and law enforcement officers regarding FISA surveillances and searches.

On May 17, 2002, the FISA Court rejected the attorney general's new policy.[20] The FISA Court ruled that law enforcement officials cannot a) direct or control an investigation using FISA searches or surveillances for law enforcement objectives, b) direct or control the use of FISA procedures to enhance a criminal prosecution, c) make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances, or d) that representatives of DOJ's Office of Intelligence Policy and Review (OIPR) be invited to ("chaperone" in the view of the DOJ) all meetings between FBI and DOJ's Criminal Division to consult regarding efforts to investigate or protect against foreign attack, sabotage, or international terrorism to ensure that foreign intelligence gathering remains the primary purpose of any FISA-authorized technique. The FISA Court's rejection of the new guidelines led to the first-ever appeal to the FISA Court of Review.

In its decision, the FISA Court of Review decided that FISA does not preclude or limit the government's use of foreign intelligence information, including evidence of crimes, in certain types of criminal prosecutions.[21] The court of review determined that the restrictions imposed by the FISA Court on the government are not required by FISA, as amended by the USA PATRIOT Act or by the Constitution and that the USA PATROIT Act amendments of the FISA statute do not violate the Fourth Amendment of the Constitution.

The court of review made several important points. First, there must be a significant foreign intelligence information-gathering

purpose for every FISA application for electronic monitoring or search, such as recruiting a foreign spy as a double agent, identification of foreign intelligence taskings, or the discovery of foreign spy tradecraft.[22]

Second, the court determined that FISA could be used to obtain evidence primarily for a criminal prosecution if the prosecution is an offense related to a foreign intelligence threat (a foreign intelligence crime) and a significant foreign intelligence-gathering purpose also is present.[23] The court defined foreign intelligence crimes as those listed in the FISA statute, including espionage, international terrorism, unlawful clandestine intelligence activities, sabotage, identity fraud offenses committed for or on behalf of a foreign power, and aiding or abetting or conspiring to commit these offenses.[24] Additionally, any ordinary crime intertwined with a foreign intelligence activity is included, such as bank robbery to finance terrorist actions or even credit card fraud to hide the identity of a spy.[25]

Finally, the court recognized that the USA PATRIOT Act lawfully breached the "wall" between criminal law enforcement and intelligence or counterintelligence gathering. Congress' intent in this matter is demonstrated amply by its addition of a new section to FISA by the USA PATRIOT Act. The new FISA Section 1806(k) reads:

> 1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with federal law enforcement officers to coordinate efforts to investigate or protect against
>
> a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

...additional safeguards are built into FISA if the target of the monitoring or search is a U.S. citizen or an alien admitted for permanent residence.

> 2) Coordination authorized under paragraph 1 shall not preclude the certification required by Section [1804](a)(7)(B) of this title or the entry of an order under Section [1805] of this title.[26]

This decision by the FISA Court of Review vindicates Congress' and the attorney general's view of FISA. It is permissible for intelligence and law enforcement officials to coordinate their efforts using all available resources, including FISA surveillances and searches, to detect, frustrate, and convict spies and terrorists.

It is important to note that additional safeguards are built into FISA if the target of the monitoring or search is a U.S. citizen or an alien admitted for permanent residence. The burden placed upon the government to obtain a FISA order is higher if the target is a U.S. person.[27] The act clearly states that the simple exercise of First Amendment rights by U.S. persons cannot be the basis for considering that person to be an agent of a foreign power.[28] The act also clearly establishes how and when information regarding a U.S. person may be used.[29]

USA PATRIOT Act and Information Sharing

An extremely important aspect of the USA PATRIOT Act is that it permits greater sharing of intelligence information between law enforcement and national security investigators, regardless of the source of the intelligence information. Section 203 of the USA PATRIOT Act amends Rule 6 of the Federal Rules of Criminal Procedure to permit the disclosure of grand jury information containing foreign intelligence information to "any federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties."[30] The reporting requirement differs in that the name of the individual receiving the information is not given to the court, only

the department or agency receiving the information. This section also amends Title III (the federal wiretap statute) to permit the same type of disclosure of intelligence information gathered during a court authorized criminal wiretap.[31]

Section 905 of the act[32] underscores the importance that Congress assigns to information sharing. That section requires the attorney general, or any head of a federal department or agency with law enforcement responsibility, to promptly disclose to the director of the CIA any foreign intelligence information gathered as a result of a criminal investigation.

Other Related Amendments

The USA PATRIOT Act amended many federal statutes in significant ways that are important to criminal and intelligence investigators. It is impossible to discuss all of these amendments in this limited space. However, some of these amendments should be mentioned.

A very significant change is that the USA PATRIOT Act makes terrorism a predicate offense allowing for a wiretap under Title III.[33] Investigators now have a choice, depending on the nature of the investigation, to apply for a FISA order or a Title III wiretap order.

In addition, the act also allows for a roving wiretap under FISA.[34] Roving wiretaps allow law enforcement to respond to time-sensitive criminal or terrorist activity by continuing court sanctioned electronic surveillance, even if the target of the surveillance rapidly switches cellular telephones, Internet accounts, or meeting venues.

USA PATRIOT Act and Pen Registers and Traps and Traces

FISA contains specific provisions regarding the use of pen registers and traps and traces in foreign intelligence investigations.[35] Section 214 of the USA PATRIOT Act changes the standard for issuing pen registers and trap and trace orders. FISA pen registers and traps and traces now can be obtained when the government certifies that the information likely to be obtained is foreign intelligence information not concerning a U.S. person or is relevant to ongoing investigations to protect against terrorism or clandestine intelligence activities.[36] Prior to the USA PATRIOT Act, pen register and trap and trace orders required showing that there was relevance to an investigation and that there was reason to believe that the targeted line was being used by an agent of a foreign power or someone in communication with such an agent under certain circumstances. The second requirement no longer exists.

> ***"...the USA PATRIOT Act makes terrorism a predicate offense allowing for a wiretap under Title III."***

The USA PATRIOT Act also amended Title III, FISA, and the federal statute related to pen registers to explicitly authorize the use of pen registers and traps and traces on communication networks other than just telephones.[37] Computer networks and cellular telephones are now specifically subject to this technique.

Criminal pen register and trap and trace orders are no longer limited to the geographic area within the jurisdiction of the issuing court.[38] All service providers necessary to the execution of the order, regardless of their location, are covered by such orders.

USA PATRIOT Act and Physical Searches

Historically, some federal courts permitted the government to search premises, but delay for a reasonable time the required notice that the government had entered the premises.[39] The USA PATRIOT Act amended federal law to statutorily recognize the practice.[40] Delayed notice, or sneak-and-peek warrants, are now permissible where the court finds reasonable cause to believe that immediate notification of the execution of the warrant would have an adverse result.[41] The warrant must prohibit the seizure of tangible property unless the court finds it necessary. The warrant also must provide for giving notice of the search within a reasonable time, but extensions of time can be granted.

The act expands the reach of search warrants in domestic and international terrorism cases.[42] Ordinarily, criminal search warrants must be issued in the districts where the searches will occur.[43] Under the new rule, however, a magistrate judge in a district "in which activities related to the terrorism may have occurred"[44] may issue a war-

rant in that terrorism investigation that can be executed within or outside that district.

It is important to note that there is a 4-year sunset provision for some parts of the act.[45] The sharing of grand jury information portion of the act does not expire as of December 31, 2005. However, the "significant purpose" certification for FISA intercepts, the provosions regarding roving FISA surveillance, and the pen register and trap and trace do.

CONCLUSION

From a national security and law enforcement perspective, the United States has made considerable progress through recent court cases and congressional action toward ensuring that threats to national security are effectively investigated and countered. At the same time, care must be taken to ensure that the new tools provided by Congress in the USA PATRIOT Act are employed within the constraints of the Constitution. The Supreme Court has said "the police must obey the law while enforcing the law, that in the end life and liberty can be as much endangered from illegal methods used to convict those thought to be criminals as from the actual criminals themselves."[46]

FISA's different standards for intelligence surveillance have been viewed suspiciously by some who fear the loss of individual liberty. Care must be taken to avoid any abuse of this tool by law enforcement. The Court has warned that "the greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."[47] Government should not overstep its bounds.

Law enforcement must act aggressively to investigate and prevent attacks from those who wish this country harm. At the same time, there must be oversight, both internal and external, to ensure that law enforcement is not overzealous. FISA and the USA PATRIOT Act provide such oversight. While the USA PATRIOT Act removed many of the obstacles that hindered terrorist and intelligence investigations in the past, it did not give law enforcement and intelligence agencies a free hand. The actions of

the government still are conducted under the watchful eye of the courts. In the end, law enforcement and intelligence investigators must be mindful that the constitutional protections that limit their authority also serve to protect their own rights as citizens of the United States. ✦

Endnotes

[1] PL 107-56, October 26, 2001, 115 Stat 272.

[2] 50 U.S.C. §§ 1801-1863(1994).

[3] Reply of the Pennsylvania Assembly to the governor, November 11, 1775.

[4] 18 U.S.C. §§ 2510-2520.

[5] 407 U.S. 297 (1972).

[6] 50 U.S.C. § 1803(b).

[7] 50 U.S.C. § 1804(a)(7)(B). Foreign intelligence information is defined as "(1) information that relates to, and if concerning a U.S. person is necessary to, the ability of the United States to protect against (a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person, is necessary to (a) the national defense or the security of the United States; or (b) the conduct of the foreign affairs of the United States." *See* 50 U.S.C. § 1801 (e).

[8] 50 U.S.C. § 1804.

[9] 50 U.S.C. § 1801 (b).

[10] 18 U.S.C. § 2518(3).

[11] 18 U.S.C. § 2518(3)(a).

[12] 18 U.S.C. § 2518(3)(b).

[13] 18 U.S.C. § 2518(3)(d).

[14] 629 F.2d 908 (4th Cir. 1980).

[15] *United States v. Falvey*, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982).

[16] *United States v. Cavanagh*, 807 F.2d 787, 791 (9th Cir. 1987), and *United States v. Duggan*, 743 F.2d 59, 73 n.5 (2d Cir. 1984)

[17] *United States v. Duggan*, 743 F.2d 59, at 78 (2d Cir. 1984) and *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987).

[18] *United States v. Megahey*, 553 F.Supp. 1180 (E.D.N.Y. 1982) *aff'd sub nom. United States v. Duggan*, 743 F.2d 59 (2nd Cir. 1984); *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987); *United States v. Badia*, 827 F.2d 1458 (11th Cir.1987), *cert. denied* 485 U.S. 937 (1988); *United States v. Johnson*, 952 F.2d 565 (1st Cir. 1991), *cert. denied* 506 U.S. 816 (1992).

[19] PL 107-56, October 26, 2001, 115 Stat 272, § 218 (amending 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)).

[20] *In re All matters Submitted to Foreign Intelligence Surveillance Court*, 218 F.Supp. 611.

[21] *In re Sealed Case*, 310 F.3d 717 (Foreign Intel. Surv. Ct. Rev., 2002).

[22] *Id.* at 736.

[23] *Supra* note 21 at 743.

[24] *Supra* note 21 at 723; 50 U.S.C. § 1801(a)-(e).

[25] *Supra* note 21 at 736.

[26] *Supra* note 21 at 733; 50 U.S.C. § 1806(k).

[27] 50 U.S.C. § 1801(b) distinguishing between agents of a foreign power who are U.S. persons and non-U.S. persons and setting out a somewhat higher standard for a U.S. person to be considered an agent of a foreign power; § 1801(e) setting out a stricter definition of foreign intelligence information where U.S. persons are involved.

[28] 50 U.S.C. § 1805(a)(3)(A); § 1824(a)(3)(A); § 1842(c)(2).

[29] 50 U.S.C. § 1801(h); § 1805(f); § 1806(a),(j); § 1821(4); § 1824(e)(4); § 1825; § 1843(c)(2); § 1845.

[30] *Supra* note 1, § 203a, amending Rule 6(e)(3)(c)(I)(V).

[31] *Supra* note 1, § 203b.

[32] *Supra* note 1, § 905.

[33] *Supra* note 1, § 201, amending 18 U.S.C. 2516(1).

[34] *Supra* note 1, § 206, amending 50 U.S.C. § 1805(c)(2)(B).

[35] 50 U.S.C. §§ 1841-1846.

[36] *Supra* note 1, § 214, amending 50 U.S.C. § 1842(c)(2).

[37] *Supra* note 1, §§ 214 and 216 (amending 50 U.S.C. §§ 1842, 1843, and 18 U.S.C. §§ 3121, 3123, and 3127)

[38] *Supra* note 1, § 216 (amending 18 § 3123; 3123(b)(1)(C) no longer requires that geographic limits be specified; however, 3127(2)(A) imposes a "nexus").

[39] *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986); *United States v. Ludwig*, 902 F.Supp. 121 (W.D. Tex. 1995); *United States v. Villegas*, 899 F.2d 1324 (2nd Cir.1990); *United States v. Pangburn*, 983 F.2d 449 (2nd Cir. 1993).

[40] *Supra* note 1, § 213, amending 18 U.S.C. § 3103a.

[41] Adverse result is defined as one resulting in endangering a life or a person's physical safety; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; serious jeopardy of an investigation or undue delay in trial; *see* 18 U.S.C. § 2705(a)(2).

[42] *Supra* note 1, § 219, amending F.R.C.P. Rule 41(b)(3). International terrorism is defined in Title 18 U.S.C. § 2331(1); domestic terrorism is defined in 18 U.S.C. § 2331(5).

[43] There is an exception to this rule for movable objects; see F.R.C.P. Rule 41(b)(2).

[44] *Supra* note 42.

[45] *Supra* note 1, § 224(a).

[46] *Spano v. New York*, 79 S. Ct. at 1206 (1959).

[47] *Olmstead v. United States*, 48 S. Ct. 564 at 572-573 (1928).

Law enforcement officers of other than federal jurisdiction who are interested in this article should consult their legal advisors. Some police procedures ruled permissible under federal constitutional law are of questionable legality under state law or are not permitted at all.

~~SECRET~~ Secret (by EC 5-7-03 E-Mail)

Memorandum

To : [redacted] b6 b7C
Assistant Attorney General
Office of Legal Policy
Department of Justice

Date 04/29/2003

DATE: 12-16-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-16-2030

From : [redacted] b6 b7C
Associate General Counsel
Office of the General Counsel

Subject : Library Usage

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] b5

ep. Dir. ____
hief of Staff ____
ff. of Gen. ____
ounsel ____
sst. Dir.: ____
Admin. Ser. ____
Crim.. Inv. ____
CJIS ____
Finance ____
Info. Res. ____
Lab. ____
National Sec. ____
OPR ____
ff. of Public & Cong. Affs. ____
Training ____
ff. of EEOA ____
irector's Office ____

1 - J. Patrick Rowan
1 - C. Steele
1 - [redacted] (PENTTBOMB UNIT) b6 b7C
1 -
1 -
DCL

Secret
~~SECRET~~

MAIL ROOM □

FBI/DOJ

b6
b7C

Memorandum from [redacted]
Re: Library Usage, 04/29/2003

Classified Secret

[redacted] (S)

b1
b2
b6
b7C
b5

If I can assist you in any other way, please contact me at [redacted] or Assistant General Counsel [redacted]

Order Code RS21472
Updated May 19, 2003

Proposed Change to the Foreign Intelligence Surveillance Act (FISA) under S. 113

Jennifer Elsea
Legislative Attorney
American Law Division

Summary

The Senate recently passed S. 113, a bill in the 108th Congress to extend the coverage of the Foreign Intelligence Surveillance Act ("FISA") to non-United States persons who engage in international terrorism or activities in preparation for international terrorism, without a showing of membership in or affiliation with an international terrorist group. FISA provides a means by which the government can obtain approval to conduct electronic surveillance (wiretap) and other searches with respect to a foreign power or its agents in order to obtain intelligence related to espionage, terrorism, or other matters involving national security.

The Foreign Intelligence Surveillance Act (FISA), P.L. 95-511, Title I, Oct. 25, 1978, 92 Stat. 1796, codified at 50 U.S.C. § 1801 *et seq.*, provides a framework for the use of electronic surveillance and other investigative methods to acquire foreign intelligence information. This measure seeks to strike a balance between national security needs in the context of foreign intelligence gathering and privacy rights guaranteed by the Fourth Amendment of the Constitution.[1] FISA provides a means by which the government can obtain approval to conduct searches and surveillance of a foreign power or its agents without first meeting the more stringent standard in Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.* [hereinafter "Title III"] that applies to criminal investigations. While Title III requires a showing of probable cause that a proposed target has committed, is committing, or is about to commit a crime, FISA requires a showing of probable cause to believe that the target is a foreign power or an agent of a foreign power.

[1] U.S. CONST. Amend. IV provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

In the aftermath of the September 11, 2001 terrorist attacks on the United States, Congress amended FISA so that it no longer requires a certification that the (primary) purpose of a search or surveillance is to gather foreign intelligence information.[2] As amended by the USA PATRIOT Act,[3] FISA requires that a "significant purpose" of the investigation be the collection of foreign intelligence information, which has been interpreted to expand the types of investigations that may be permitted to include those in which the primary purpose may be to investigate criminal activity, as long as there is at least a measurable purpose related to foreign intelligence gathering.[4] The proposed change under S. 113 would remove the requirement for the government to show that the intended target is associated with a foreign power, as long as the intended target is not a U.S. person.

The bill was introduced in the 107th Congress as S. 2586 (known as the Schumer-Kyl Bill). In its original form, it would have amended the definition of "foreign power"[5] to include (4) *any person, other than a United States person, or* group that is engaged in international terrorism or activities in preparation therefor [proposed new language in S. 2586 emphasized]. The Senate Select Committee on Intelligence held hearings on the bill on July 31, 2002,[6] but the bill never reached a floor vote. Re-introduced in the 108th Congress as S. 113, the bill was amended in committee to retain the existing definition of "foreign power," but to add a new subparagraph (c) to the definition of "agent of a

---

[2] *See* CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance.* "Foreign Intelligence Information" is defined in 50 U.S.C. § 1801(e) to mean:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

[3] P.L. 107-56 § 218.

[4] *See In re* Sealed Case, 310 F.3d 717, 735 (F.I.S.Ct.Rev. 2002) ("The addition of the word "significant" to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.").

[5] "Foreign power" is defined in 50 U.S.C. § 1801(a) to mean:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons; or
>
> (6) an entity that is directed and controlled by a foreign government or governments.

[6] Amending FISA: Hearings before the Senate Select Committee on Intelligence, July 31, 2002 (hereinafter "FISA Hearing"), *available at* [http://intelligence.senate.gov/0207hrg/020731/witness.htm].

foreign power"[7] in 50 U.S.C. § 1801(b)(1) (which excludes United States persons[8]). The amendment would add non-U.S. persons[9] who "engage[] in international terrorism or activities in preparation therefor"to the definition of "agents of a foreign power" for the purposes of FISA. Both the original proposal and the amended language appear to reach the same result: a FISA warrant would be available to investigate a non-U.S. person who engages in international terrorism or activities in preparation therefore without a requirement that there is reason to believe the person is acting on behalf of a terrorist organization, a foreign country, or any entity fitting the definition of "foreign power." The new definition would sunset with certain other provisions added in P.L. 107-56 on December 31, 2005.[10]

The bill's sponsor says an amendment is necessary to fight foreign terrorists because it is sometimes difficult to show that a proposed target is associated with a foreign power. The new definition would allow the FBI to conduct surveillance on persons who might otherwise evade surveillance through a "loophole"in the present law:

---

[7] "Agent of a foreign power" is currently defined in 50 U.S.C. § 1801(b) to mean:

(1) any person other than a United States person, who —

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who —

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

[8] "United States person" is defined in 50 U.S.C. § 1801(i) to mean:

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

[9] "Person" is defined in 50 U.S.C. § 1801(m) to mean:

any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

[10] P.L. 107-56 § 224.

> the terrorist who is either acting on his own or the terrorist who, while acting on behalf of an international terrorist organization or state, has not yet clearly signalled that to our law enforcement officials to the point that we can succeed in getting a FISA warrant.[11]

The case of Zacarias Moussaoui is advanced as a case in point. Although he is a foreign person who was engaged in suspicious activity, the FBI did not approve a request to seek a FISA application to search his computer hard drive because it could not connect him with a foreign government or specific foreign terrorist organization.[12] Some argue that the FBI's misinterpretation of the requirements of FISA, rather than defects in the statute itself led to the failure of the FBI to seek a FISA warrant.[13] Under this view, the FBI had sufficient information about Moussaoui's connections with Chechen rebels to acquire a FISA warrant, but deciding officials construed FISA to require proof of an association with Al Qaeda or another organization officially listed as a terrorist organization by the State Department.[14] Others interpret the statute to require no certification that the proposed target is associated with any specific group, inasmuch as a "group" of terrorists covered by current law might be as small as two or three persons.[15]

The Justice Department supported S. 2586, asserting that the amendment would enable the FBI to target the new type of terrorist threat faced by the United States today. An FBI official describes the new threat, that of the "international Jihad movement" thus:

> Historically, terrorism subjects of FBI investigation have been associated with terrorist organizations. As a result, FBI has usually been able to associate an individual with a terrorist organization pled, for FISA purposes, as a foreign power. To a substantial extent, that remains true today. However, we are increasingly seeing terrorist suspects who appear to operate at a distance from these organizations. In perhaps an oversimplification, but illustrative nevertheless, what we see today are (1) agents of foreign powers in the traditional sense who are associated with some organization or discernible group, (2) individuals who appear to have connections with multiple terrorist organizations but who do not appear to owe allegiance to any one of them, but rather owe allegiance to the international Jihad movement and (3)

---

[11] CONG. REC. S10426 (daily ed. Oct. 15, 2002) (statement of Senator Kyl with respect to S. 2586, 107th Congress).

[12] *See id.* Whether a timely search of Moussaoui's computer data would have revealed information that might have allowed the government to prevent the Sept. 11, 2001 attacks is a matter open to debate. *See* FISA Hearing, *supra* note 6 (Testimony of Jerry Berman, Executive Director, Center for Democracy and Technology)[hereinafter "Berman Testimony"], *available at* [http://www.cdt.org/testimony/020731berman.shtml].

[13] *See id.*; Beverley Lumpkin, *The 'Lone Wolf,'* ABC News Online, Aug. 2, 2002, *at* [http://abcnews.go.com/sections/us/HallsOfJustice/hallsofjustice133.html].

[14] *See* Senators Patrick Leahy, Charles Grassley, and Arlen Specter, *Interim Report: FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures*, at 23 -25, Feb. 2003 [hereinafter "Interim Report"](concluding that FBI officials misapplied the FISA standards for determining whether there was reason to believe Moussaoui was an agent of a foreign power); *Hill Probers Upgrade Evidence Gathered From Moussaoui*, WASH. POST, June 6, 2002, at A18 (reporting reason given by officials for rejecting Minneapolis FBI agent's request for a FISA warrant to search Moussaoui's computer hard drive).

[15] *See* H.R.Rep. 95-1283, at pt. 1, 74 and n. 38 (1978).

individuals who appear to be personally oriented toward terrorism but with whom there is no known connection to a foreign power.[16]

Accordingly, including individuals engaging in terrorist activities or preparations therefore under the definition of "agent of a foreign power" would allow investigators to use FISA to pursue the "lone wolf" terrorist, without the need to show any association to a foreign terrorist group or other foreign power. To treat a United States person as an agent of a foreign power would continue to require a showing that the person is working for or on behalf of a foreign power.[17] In order to obtain a FISA warrant to conduct searches or surveillance with respect to a non-U.S. person as an "agent of a foreign power" under the proposed language, probable cause to believe that the proposed target is engaged or will engage in an act of international terrorism[18] would be required. Critics argue that in the event such evidence is already available, there would be no reason to treat it as anything other than a criminal matter, for which a Title III warrant would be appropriate.[19] Additionally, some question whether there is any rational purpose for treating foreign "lone wolf" terrorists under a separate legal regime from that which applies to "lone wolf" terrorists who are U.S. citizens or permanent resident aliens.[20] The Fourth Amendment has been interpreted to cover non-U.S. persons in the United States who are suspected of involvement in criminal activity. Under this view, there is no constitutional reason for treating U.S. persons and non-U.S. persons differently where there is no suspicion of association with a foreign terrorist organization or other foreign power. Some believe, therefore, that the amendment raises significant constitutional issues.[21]

It has also been argued that to divorce FISA from the purpose of gathering foreign intelligence information about foreign powers and their agents, as those terms are normally understood, is a significant departure from the original purpose of the statute and part of the reason courts have held that searches under FISA do not violate the Fourth

---

[16] *See* FISA Hearing, *supra* note 6 (Statement for the Record of Marion E. (Spike) Bowman, Deputy General Counsel, Federal Bureau of Investigation).

[17] 50 U.S.C. § 1801(b)(2)(C).

[18] "International terrorism" is defined by 50 U.S.C. § 1801(c) to mean activities that —

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended —

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

[19] *See* Berman Testimony, *supra* note 12.

[20] *See id.*

[21] *See id;* Letter from Kate Martin, Director, Center for National Security Studies, *Proposed Amendments to Foreign Intelligence Surveillance Act*, July 31, 2002.

Amendment.[22] The new proposed added definition for "agent of a foreign power" would also broaden other definitions in the statute that are tied to it. For example, "foreign intelligence information" under 50 U.S.C. § 1801(e) would include "information that relates to ... the ability of the United States to protect against ... actual or potential attack or other grave hostile acts of" an individual non-U.S. person suspected of terrorism but unaffiliated with a foreign power, as defined; and "sabotage or international terrorism" committed by same.

On the other hand, the bill's proponents argue that the new definition, by requiring probable cause that the target is engaging in or preparing for terrorist activity that transcends international boundaries, already meets a high enough standard of particularity to satisfy Title III and constitutional standards.[23] They believe that the interest that the courts have identified to justify the procedures of FISA are not likely to differ appreciably between a case involving a single terrorist and a case involving a group of two or three terrorists, who may be treated as a "foreign power" under existing law.[24] Furthermore, the Justice Department argues that the magnitude of harm presented by international terrorists justifies a different set of parameters for determining whether a search is "reasonable" under the Fourth Amendment, which depends on an analysis of whether the government's interests outweigh any intrusion into individual privacy interests.[25] In light of the efforts of international terrorists to obtain weapons of mass destruction, it is argued, a terrorist whose ties to an identified "group" remain obscure presents a grave danger to the United States that outweigh the minimal privacy interests likely to be impacted by the proposed change.

As amended prior to passage in the Senate, S. 113 would require the Attorney General to submit an annual report, in addition to reports already required under FISA, describing the number of times the new authority is used, according to the types of searches or seizures that are conducted, the number of times information obtained through these uses is approved for use by prosecutors in a criminal trial, and any significant court interpretations of the new language that may follow. An amendment that, rather than defining non-United States persons engaging in international terrorism to *be* agents of a foreign power, would have permitted a *presumption* that such persons are agents of a foreign power, was not agreed to.

---

[22] *See* Berman Testimony, *supra* note 12. *Cf.* United States v. United States District Court, 407 U.S. 297, 308 (1972) (differentiating a domestic intelligence surveillance from a foreign intelligence case because it "require[d] no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country"); *In re Sealed Case,* 310 F.3d at 746 (same).

[23] *See* CONG. REC. S10426-28 (daily ed. Oct. 15, 2002) (statement of Senator Kyl with respect to S. 2586 of the 107th Congress).

[24] *See id.* at S10430 (citing letter from Daniel J. Bryant, Assistant Attorney General, Department of Justice, Office of Legislative Affairs to Senators Kyl and Schumer).

[25] *See* FISA Hearing, *supra* note 6 (Statement for the Record of Marion E. (Spike) Bowman, Deputy General Counsel, Federal Bureau of Investigation), *reprinted at* CONG. REC. S10430-32 (daily ed. Oct. 15, 2002).

~~SECRET~~

Rowan, J Patrick

From: [redacted]
Sent: Monday, August 04, 2003 9:06 AM
To: Rowan, J Patrick; [redacted] BOWMAN, MARION
Subject: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2
b6
b7C
b5

DATE: 01-03-2006
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 01-03-2031

Pat/Spike [redacted]

[redacted]

b6
b7C
b5

-----Original Message-----
From: [redacted]
Sent: Monday, August 04, 2003 9:04 AM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

b2
b6
b7C
b5
b1

(S)

[redacted]

(S)

b1
b2
b6
b7C
b5

[redacted] Spike and Pat Rowan [redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Saturday, August 02, 2003 12:17 PM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

b2
b6
b7C
b5
b1

(S)

(S)

[redacted]

(S)

~~SECRET~~

(S)

-----Original Message-----
From:
Sent: Thursday, July 31, 2003 9:57 AM
To:
Cc:
Subject:

b2
b5
b6
b7C
b1

(S)

(S)

(S)

(S)

(S)

(S)

Investigative Law Unit
Office of the General Counsel

~~SECRET~~

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 30, 2003

DATE: 01-03-2006
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 01-03-2031

To: File

From: [redacted] b6 b7C

Re: FISA Pen Registers and the Definition of "Content"

On today's date, I had another installment of an ongoing conversation with Spike Bowman concerning the definition of "content" in the context of pen registers sought pursuant to the authority of the Foreign Intelligence Surveillance Act ("FISA"). [redacted] (S) [redacted] (S) b1

In short, in a soon to be prepared memorandum on the issue, I will address the discrepancy between the FISA definition of "content" and the definition of content found in the Electronic Communications Privacy Act. *Compare* 50 U.S.C. Section 1801(n) *with* 18 U.S.C. Section 2510(8). That memorandum will conclude that, while anomalous, the current FISA definition of content includes, among other things, the "existence" of the communication and "any information concerning the identity of the parties."

[redacted] (S) b1 b6 b7C

My purpose in conferring today with Spike was to confirm my understanding that while we have an awkward statutory construct that leads us to rely upon a criminal statutory provision to get to the correct Constitutional result, we do not today have any legal or ethical impediments to

[redacted] (S) b1 b6 b7C

With regard to resolution of the nagging statutory problem and its practical consequences for, among other things, appropriate dissemination of gathered pen register information, I will be conferring later today with Technology Law Branch attorney [redacted] and, thereafter, technical guru [redacted] to further educate myself on the issue. b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~ b6
b7C

Rowan, J Patrick

From: [redacted]
Sent: Thursday, August 21, 2003 5:17 PM
To: Rowan, J Patrick
Subject: **~~SECRET~~* [redacted] Pen Registers and The OLC (S)

DATE: 12-15-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-15-2030

b1

Pat:

In response to your request, I think we can state it fairly succinctly. [redacted]

b5

[redacted] (S) b1

Finally, linking the word [redacted] is classified. Describing the function of the program without the name, however, is unclassified. Hope this helps. I am out of here to the beach. See you after Labor Day. [redacted]

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

~~SECRET~~

Rowan, J Patrick

From: Rowan, J Patrick
Sent: b6 Thursday, August 21, 2003 4:05 PM
To: b7C
Cc: BOWMAN, MARION E.;
Subject: RE: Fun Facts About Pen Registers

DATE: 12-15-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-15-2030

I spoke to about this briefly. I will call over to OLC about an opinion, but I am hoping that you can assist me by putting together two or three paragraphs that I will use to make the request. It does not need to be polished; I am going to use it to make the call, and if they ask for something in writing, we can polish it.

(S) b1 b5

-----Original Message-----
From: b6
Sent: Wednesday, August 20, 2003 3:22 PM b7C
To:
Cc: Rowan, J Patrick; BOWMAN, MARION E.;
Subject: Fun Facts About Pen Registers

b6 b1
(S) b7C b5

Following up on yesterday's discussion, I spoke earlier today with progam manager for th operated out of the Electronic Communications Analysis Unit. A summary of that discussion is attached. As (S)

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

<< File pen.wpd ->

~~SECRET~~

SECRET

Rowan, J Patrick

From: [redacted]
Sent: Wednesday, August 20, 2003 3:22 PM
To: [redacted]
Cc: Rowan, J Patrick; BOWMAN, MARION E.; [redacted]
Subject: Fun Facts About Pen Registers

DATE: 12-15-2005
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-15-2030

b6
b7C

(S) [redacted] (S)

Following up on yesterday's discussion, I spoke earlier today with [redacted] progam manager for th[redacted] perated out of the Electronic Communications Analysis Unit. A summary of that discussion is attached. As [redacted]

[redacted]pen.wpd
(11 KB)

b1
b5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SECRET

Rowan, J Patrick

From:
Sent: Wednesday, September 03, 2003 1:56 PM
To: b6
Cc: b7C Rowan, J Patrick;
Subject: Re: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

OGC.

As noted in our prior e-mail

Unless OGC objects, will begin this project in the near future.

b2 b2 b7E b7E b5 b6 b7C b5

SSA Office of Division Counsel

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED DATE 12-15-2005 BY 65179/DMH/LP/RW 05-cv-0845

Privileged and ~~Confidential~~

>>> 09/03 10:48 AM >>>

Thanks for your response; my info. agrees with yours-

and have these substantive matters;

b2 b7E b6 b7C b5

b2

b6

Let me know what you need from me--SA researched this problem in February or so, and we recommended that

b7C b2 b7E b5

Thank you,

09/02 9:36 AM

There is no reason not to since FISA info is readily avail in ACS.

>>> 09/02 6:45 PM >>>

b2 b7E b6 b7C b5

Any word about the FISA-derived information yet?
Thanks,

b6
b7C

>> [redacted] 08/29 2:33 PM >>>
Many offices do [redacted] OGC has previously taken the position that [redacted]

>>> [redacted] 08/29 2:18 PM >>> b6
TO: [redacted] Rowan, [redacted] OGC b7C
[redacted] OGC

RE: [redacted] b5

[redacted] requests that OGC provide guidance regarding [redacted]

[redacted] requests that OGC review and comment on this issue. b2 b7E

SSA [redacted] b5
[redacted] Office of Division Counsel [redacted]
b6
Privileged and ~~Confidential~~
b7C

>>> [redacted] 08/22 8:36 AM >>>
[redacted] Analyst [redacted] worked with the TO people and determined it is possible to do, it just isn't done. [redacted] b6 b7C

Questions: b2 b7E b5

[redacted]

Please respond when you have a chance.
Thank you, b6 b7C b2 b7E b5

[redacted]

Rowan, J Patrick

From:
Sent: Friday, August 29, 2003 2:18 PM
To: Rowan, J Patrick; BOWMAN, MARION E.
Cc:
Subject: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

TO: Rowan, OGC
ILU, OGC

RE:

requests that OGC provide guidance regarding

requests that OGC review and comment on this issue.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-15-2005 BY 65179/DMH/LP/RW 05-0845

SSA
Office of Division Counse

Privileged and Confidential

>>> 08/22 8:36 AM >>>

Analyst worked with the TO people and determined it is possible to do, it just isn't done.

Questions:

Please respond when you have a chance.
Thank you,

b2
b6
b7C
b7E
b5

b6
b7C

Rowan, J Patrick

From:
Sent: Wednesday, September 03, 2003 2:43 PM
To:
Cc: Rowan, J Patrick;
Subject: RE: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

b6
b7C

- I spoke with and OGC poses no objection to loading FISA as long as the information is flagged as FISA derived.

b2
b7E

-----Original Message-----
From:
Sent: Wednesday, September 03, 2003 1:56 PM
To:
Cc:
Rowan, J Patrick;
Subject: Re: REQUEST FOR OGC OPINION - FISA-PEN UPLOAD INSTRUCTIONS

b6
b7C

OGC.

As noted in our prior e-mail -

Unless OGC objects, will begin this project in the near future.

b2
b7E
b5

Office of Division Counsel

b2
b6
b7C

Privileged and ~~Confidential~~

b5

>>> 09/03 10:48 AM >>>

Thanks for your response; my info agrees with yours

and have those substantive matters.

b2
b7E
b6
b7C
b5

Let me know what you need from me--SA researched this problem in February or so, and we recommended that

b2
b7E

Thank you,

b6
b7C
b5

There is no reason not to since FISA info is readily avail in ACS.

09/02 6:45 PM >>>

Any word about the FISA-derived information yet?
Thanks,

>>> 08/29 2:33 PM >>>

>>> 08/29 2:18 PM >>>
TO: Rowan, OGC
OGC

RE:

requests that OGC provide guidance regarding

requests that OGC review and comment on this issue.

SSA Office of Division Counsel

Privileged and ~~Confidential~~

>>> 08/22 8:36 AM >>>

. Analyst worked with the TO people and determined it is possible to do, it just isn't done.

Questions:

Please respond when you have a chance.
Thank you,

b2
b7E
b6
b7C
b5

TOOLS USED ON THE INTELLIGENCE SIDE

A. FISAs: For searches & surveillance

1. Legal Standard: Probable cause to believe that:

(1) the target is a foreign power or an agent of a foreign power

(2) that facilities/places at which surveillance is directed is being used, or about to be used, by a foreign power or agent of foreign power

2. "Agent of a foreign power" includes a person who engages in sabotage or international terrorism, or acts in preparation, for or on behalf of a foreign power

3. "Foreign Power" includes a group engaged in international terrorism

B. National Security Letters (NSLs)

1. Analog to criminal subpoenas

2. Used to obtain:

a. Telephone and electronic communications records from telephone companies & ISPs

b. Records from financial institutions

c. Information from credit bureaus

3. USA-Patriot Act expanded our ability to use

-- Eliminated requirement to show by specific & articulate facts that target was "agent of foreign power"

-- Now only requires relevance to a national security investigation

-- Lowered approval levels to SACs (used to be HQ or ADIC)

C. FISA Pen Registers/Trap & Trace Orders

1. New Act also made these easier

-- Again eliminated "agent of foreign power" test

-- Relevance only

USA-Patriot Act: "Uniting + Strengthening America By Providing Appropriate Tools Required to Intercept + Obstruct Terrorism"

D. FISA Business Records Orders

1. Used to cover only 4 categories (common carriers, public accomodations, vehicle rentals, storage facilities)

2. Now covers all business records

3. Also changed standard to simple relevance

e) The name, title and address of the communication service provider who should receive the request.

B. (U) Telephone subscriber and toll records acquired by the foregoing means may be disseminated to other agencies of the Federal Government only when such information is clearly relevant to their authorized responsibilities. *See: id. Section 2709(d).*

C. (U) On a semiannual basis, the FBI must fully inform the House Permanent Select Committee on Intelligence; the House Committee on the Judiciary; the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary; of requests made by the foregoing means. *See: id. Section 2709(e).*

Section 3-04 (U) Pen Registers and Trap and Trace Devices

A. (U) Generally, applications for pen registers and trap and trace devices must be submitted to the FISA Court, or to specially designated Federal Magistrates. All such applications must include:

1. The identity of the Federal officer making the application;
2. A certification that the information likely to be obtained is foreign intelligence information not concerning an a USPER; or is relevant to an authorized investigation to protect against IT or clandestine intelligence activities, provided that such an investigation of an USPER is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution;
3. Information which demonstrates a reason to believe that the target telephone line, communication instrument or device has been, or is about to be used in communication with: an individual who has or is engaging in international terrorism or clandestine intelligence activities which violate U.S. criminal law; or a foreign power or agent thereof which is engaged in international terrorism or clandestine intelligence activities which violate U.S. criminal law.

B. (U) Court Orders approving pen registers and trap and trace devices, authorize their installation and operation for periods not to exceed 90 days. Extensions of additional 90 day periods may be obtained.

C. (U) Notwithstanding the foregoing, however, whenever the Attorney General determines that an emergency exists, and that factual bases exist for a Court Order, the Attorney General may authorize the execution of an emergency pen register or trap and trace device; if the Court is informed at the time of the authorization, and application is in fact made no more than 48 hours after the authorization.

1. Authorized emergency pen registers and trap and trace devices shall terminate when the information sought is obtained, when the application is denied, or 48 hours after the authorization is given, whichever comes first.
2. If a Court Order is denied after an emergency pen register or trap and trace device has been installed, no information collected as a result shall be used in any manner, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

D. (U) Notwithstanding the foregoing, the President, acting through the Attorney General, may also authorize the use of a pen register or trap and trace device, without a Court Order, for a

period not to exceed 15 calendar days, following a declaration of war by Congress. *See: Title 50, U.S. Code, Sections 1842-1844.*

Section 3-05 (U) Unconsented Electronic Surveillances

A. (U) The following requirements pertain to the acquisition, retention and dissemination of nonpublic available communications and other information resulting from NFIP ELSURs on foreign powers, and USPER and non-USPER Agents of foreign powers.

B. (U) Generally, applications for NFIP ELSURs must be submitted to the FISA Court. All such applications must include:

1. The identity of the Federal officer making the application;
2. The approval of the Attorney General, and the President's authority for that approval;
3. The identity or description of the target of the surveillance;
4. A statement of the facts which have led to the belief that: (i) the target is a foreign power or an agent of a foreign power, and that (ii) each of the facilities or places at which the surveillance will be directed is being used, or is about to be used by a foreign power or an agent of a foreign power;
5. A statement of proposed minimization procedures *(see: In the Matter of the Application of the U.S. for an Order Authorizing ELSUR of a Foreign Power, In the Matter of the Application of the U.S. for an Order Authorizing ELSUR of an USPER Agent of a Foreign Power and In the Matter of the Application of the U.S. for an Order Authorizing ELSUR of a Non-USPER Agent of a Foreign Power)*;
6. A statement of the nature of the foreign intelligence sought, and the types of communications or activities to be surveilled;
7. A certification by the Assistant to the President for National Security Affairs (or some other presidentially-designated Executive Branch official) that: (i) the certifying official believes the information sought to be foreign intelligence information, (ii) the purpose of the surveillance is to obtain foreign intelligence information, (iii) such information cannot reasonably be obtained by normal investigative techniques; (iv) designates the information sought per set categories and (v) includes a statement explaining the basis for the certification;
8. A statement of the means by which the surveillance will be effected and whether physical entry is required;
9. A statement of the facts concerning all previous applications that have been made involving any of the persons, facilities, or places specified in the application and the actions taken on each previous application;
10. A statement of the period of time for which the surveillance is required and (if the nature of the intelligence gathering is such that approval should not automatically terminate when the described type of information has first been obtained) a description of the facts supporting the belief that additional information of the same type will be obtained thereafter; and
11. Should more than one electronic, mechanical or other device be used with respect to a particular surveillance, a statement regarding the coverage of the devices involved and

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 153
Page 104 ~ Referral/Direct
Page 105 ~ Referral/Direct
Page 106 ~ Referral/Direct
Page 107 ~ Referral/Direct
Page 108 ~ Referral/Direct
Page 109 ~ Referral/Direct
Page 110 ~ Referral/Direct
Page 111 ~ Referral/Direct
Page 112 ~ Referral/Direct
Page 113 ~ Referral/Direct
Page 114 ~ Referral/Direct
Page 115 ~ Referral/Direct
Page 116 ~ Referral/Direct
Page 117 ~ Referral/Direct
Page 118 ~ Referral/Direct
Page 119 ~ Referral/Direct
Page 120 ~ Referral/Direct
Page 121 ~ Referral/Direct
Page 122 ~ Referral/Direct
Page 123 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 128 ~ Referral/Direct
Page 129 ~ Referral/Direct
Page 130 ~ Referral/Direct
Page 131 ~ Referral/Direct
Page 132 ~ Referral/Direct
Page 133 ~ Referral/Direct
Page 134 ~ Referral/Direct
Page 135 ~ Referral/Direct
Page 136 ~ Referral/Direct
Page 137 ~ Referral/Direct
Page 138 ~ Referral/Direct
Page 139 ~ Referral/Direct
Page 140 ~ Referral/Direct
Page 141 ~ Referral/Direct
Page 142 ~ Referral/Direct
Page 143 ~ Referral/Direct
Page 144 ~ Referral/Direct
Page 192 ~ Referral/Direct
Page 193 ~ Referral/Direct
Page 207 ~ Referral/Direct

Page 208 ~ Referral/Direct
Page 317 ~ Referral/Direct
Page 318 ~ Referral/Direct
Page 319 ~ Referral/Direct
Page 320 ~ Referral/Direct
Page 394 ~ Referral/Direct
Page 395 ~ Referral/Direct
Page 396 ~ Referral/Direct
Page 397 ~ Referral/Direct
Page 398 ~ Referral/Direct
Page 399 ~ Referral/Direct
Page 400 ~ Referral/Direct
Page 401 ~ Referral/Direct
Page 402 ~ Referral/Direct
Page 403 ~ Referral/Direct
Page 404 ~ Referral/Direct
Page 405 ~ Referral/Direct
Page 406 ~ Referral/Direct
Page 407 ~ Referral/Direct
Page 408 ~ Referral/Direct
Page 409 ~ Referral/Direct
Page 410 ~ Referral/Direct
Page 411 ~ Referral/Direct
Page 412 ~ Referral/Direct
Page 413 ~ Referral/Direct
Page 414 ~ Referral/Direct
Page 415 ~ Referral/Direct
Page 416 ~ Referral/Direct
Page 417 ~ Referral/Direct
Page 418 ~ Referral/Direct
Page 419 ~ Referral/Direct
Page 420 ~ Referral/Direct
Page 421 ~ Referral/Direct
Page 422 ~ Referral/Direct
Page 423 ~ Referral/Direct
Page 424 ~ Referral/Direct
Page 425 ~ Referral/Direct
Page 426 ~ Referral/Direct
Page 427 ~ Referral/Direct
Page 428 ~ Referral/Direct
Page 429 ~ Referral/Direct
Page 430 ~ Referral/Direct
Page 431 ~ Referral/Direct
Page 432 ~ Referral/Direct
Page 433 ~ Referral/Direct
Page 434 ~ Referral/Direct
Page 435 ~ Referral/Direct
Page 436 ~ Referral/Direct
Page 437 ~ Referral/Direct
Page 438 ~ Referral/Direct
Page 439 ~ Referral/Direct

Page 440 ~ Referral/Direct
Page 441 ~ Referral/Direct
Page 442 ~ Referral/Direct
Page 443 ~ Referral/Direct
Page 444 ~ Referral/Direct
Page 445 ~ Referral/Direct
Page 446 ~ Referral/Direct
Page 447 ~ Referral/Direct
Page 448 ~ Referral/Direct
Page 449 ~ Referral/Direct
Page 450 ~ Referral/Direct
Page 451 ~ Referral/Direct
Page 452 ~ Referral/Direct
Page 453 ~ Referral/Direct
Page 454 ~ Referral/Direct
Page 455 ~ Referral/Direct
Page 456 ~ Referral/Direct
Page 457 ~ Referral/Direct
Page 458 ~ Referral/Direct
Page 459 ~ Referral/Direct
Page 460 ~ Referral/Direct
Page 461 ~ Referral/Direct
Page 462 ~ Referral/Direct
Page 1020 ~ Duplicate
Page 1021 ~ Referral/Direct
Page 1022 ~ Referral/Direct
Page 1023 ~ Referral/Direct
Page 1024 ~ Referral/Direct
Page 1025 ~ Referral/Direct
Page 1026 ~ Referral/Direct
Page 1027 ~ Referral/Direct
Page 1028 ~ Referral/Direct
Page 1029 ~ Referral/Direct
Page 1030 ~ Referral/Direct
Page 1031 ~ Referral/Direct
Page 1032 ~ Referral/Direct
Page 1033 ~ Referral/Direct
Page 1034 ~ Referral/Direct
Page 1035 ~ Referral/Direct
Page 1036 ~ Referral/Direct
Page 1037 ~ Referral/Direct
Page 1038 ~ Referral/Direct
Page 1039 ~ Referral/Direct
Page 1040 ~ Referral/Direct
Page 1041 ~ Referral/Direct
Page 1042 ~ Referral/Direct
Page 1043 ~ Referral/Direct
Page 1044 ~ Referral/Direct
Page 1045 ~ Referral/Direct
Page 1072 ~ b1, b5, b6, b7C
Page 1073 ~ b1, b5, b6, b7C

Page 1074 ~ b1, b5, b6, b7C
Page 1075 ~ b1, b5, b6, b7C
Page 1076 ~ b1, b5, b6, b7C
Page 1077 ~ b1, b5, b6, b7C
Page 1078 ~ b1, b5, b6, b7C
Page 1079 ~ b1, b5, b6, b7C
Page 1080 ~ b1, b5, b6, b7C

SECTION-BY-SECTION

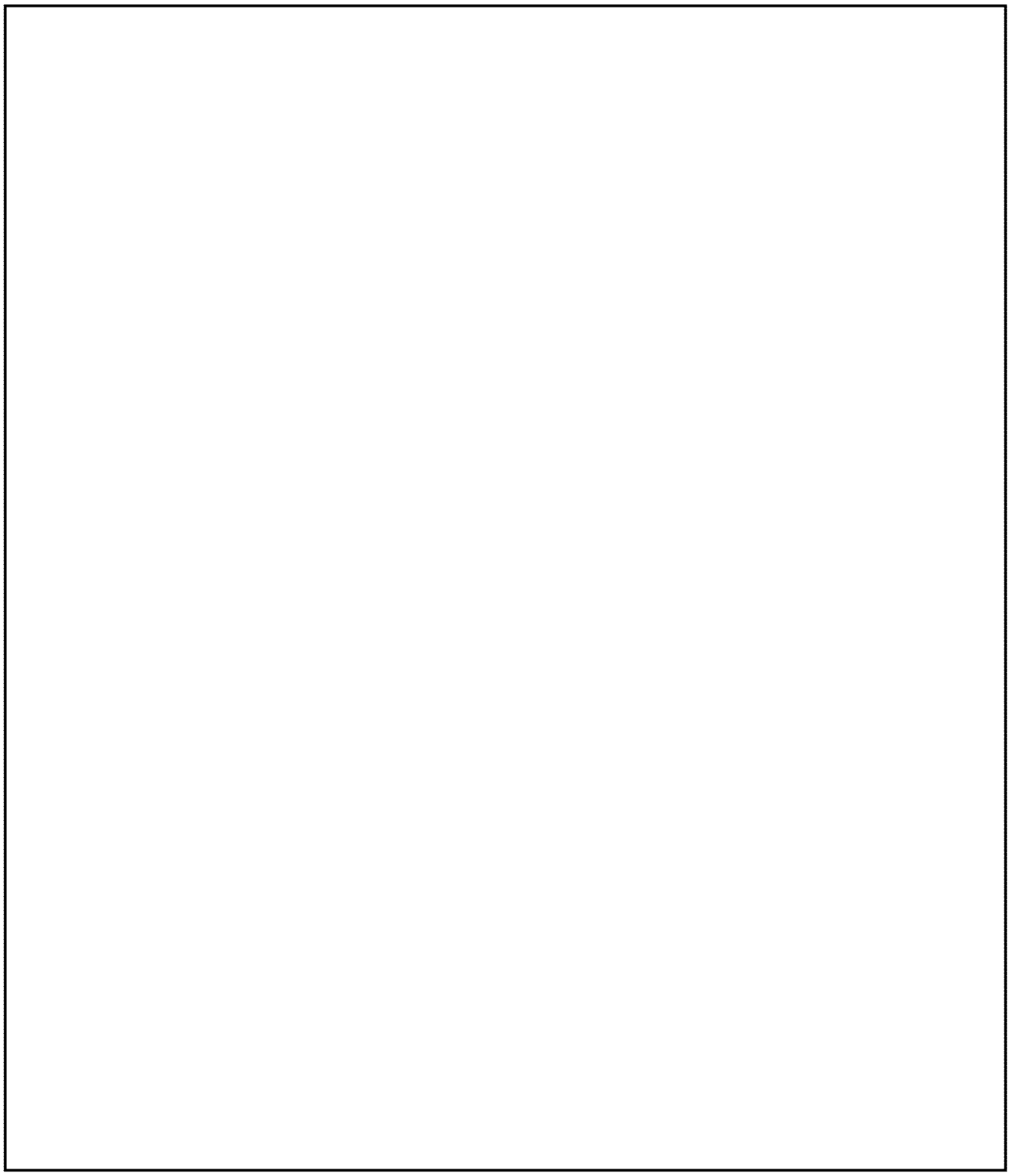
Section 1. Short Title

This section provides that this Act may be cited as the "FISA Improvements Act of 2005."

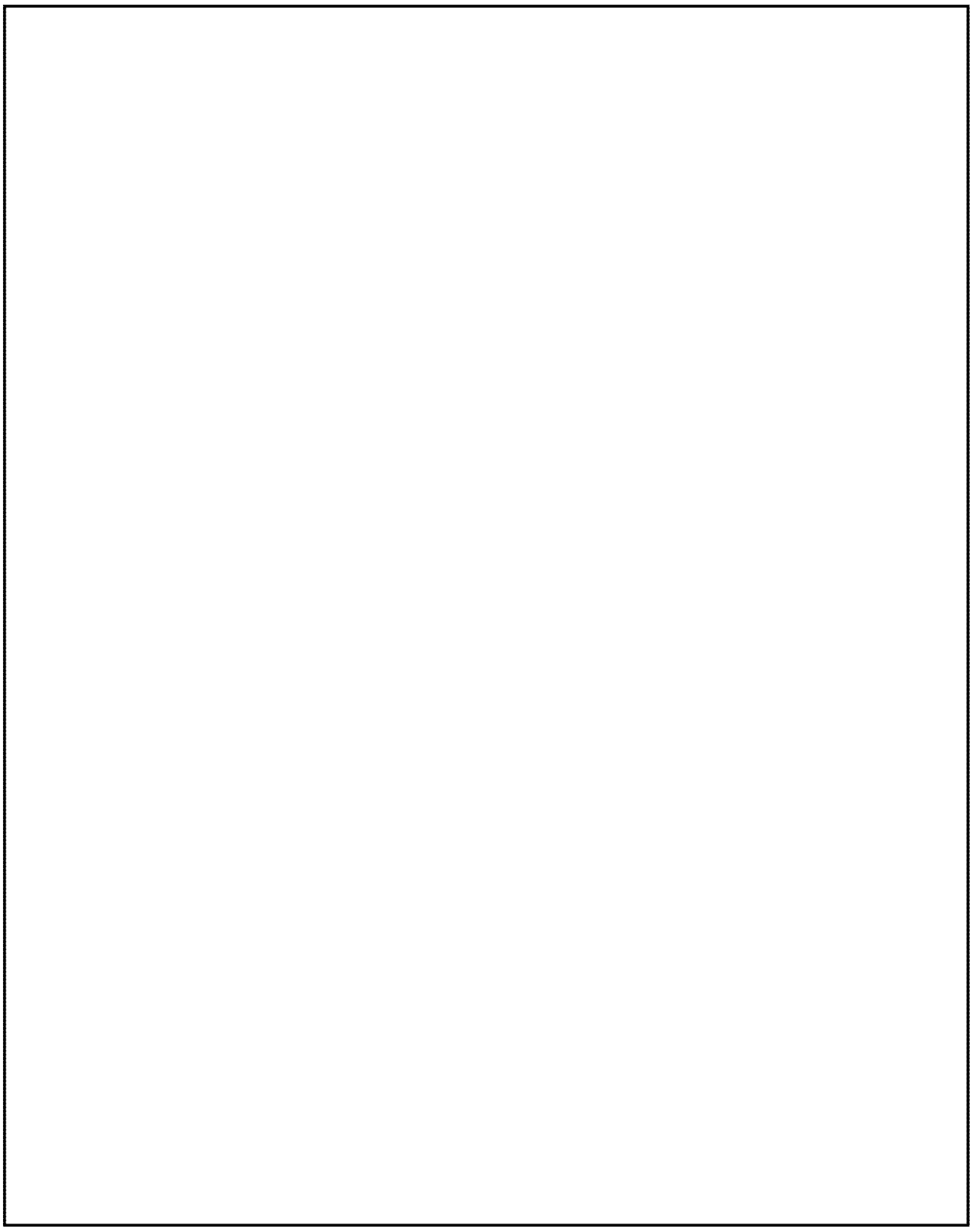
Section 2. Duration of FISA Surveillance of Non-United States Persons

Before passage of the USA PATRIOT Act, FISA orders for electronic surveillance targeted against agents of a foreign power had a maximum duration of 90 days and could be extended in 90-day increments, and orders for a physical search could be issued for no more than 45 days, unless the target was a foreign power (in which case, the order could be issued for one year.) *See* 50 U.S.C. §§ 1805(e) and 1824(d) (2000). Section 207 of the USA PATRIOT Act allows orders for physical searches to be issued for certain agents of foreign powers, including United States persons, for 90 days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and agents of foreign powers that are not United States persons. This section would extend the maximum duration of orders for electronic surveillance and physical search targeted against all agents of foreign powers who are not United States persons. Specifically, initial orders authorizing searches and electronic surveillance would be for periods of up to 120 days, and renewal orders would extend for periods of up to one year.

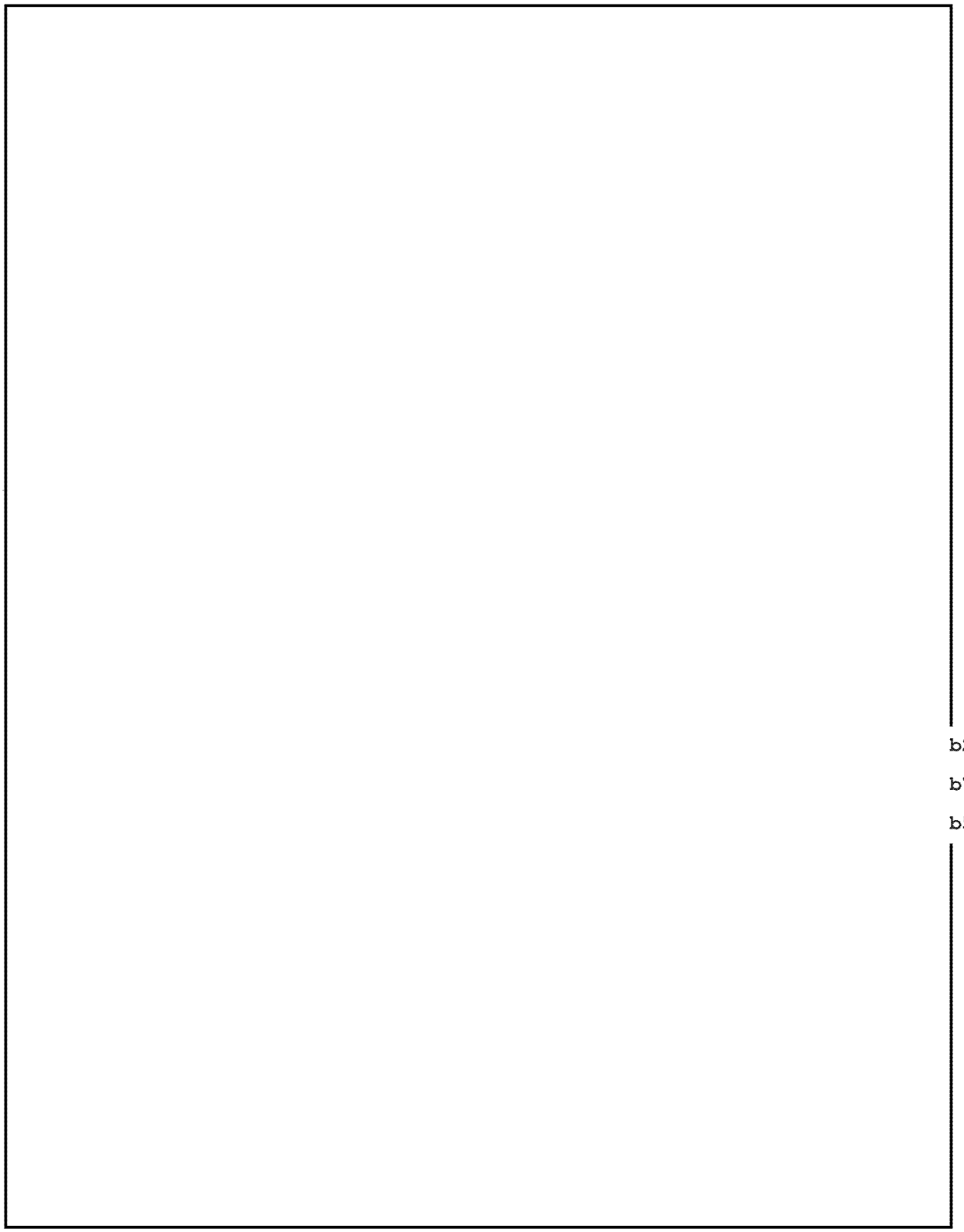
The USA PATRIOT Act did not amend the permissible duration of orders for pen register/trap and trace surveillance under FISA. The current duration of initial and renewal orders for installation and use of a pen register or trap and trace device is for a period not to exceed 90 days. This section would extend the maximum duration of both



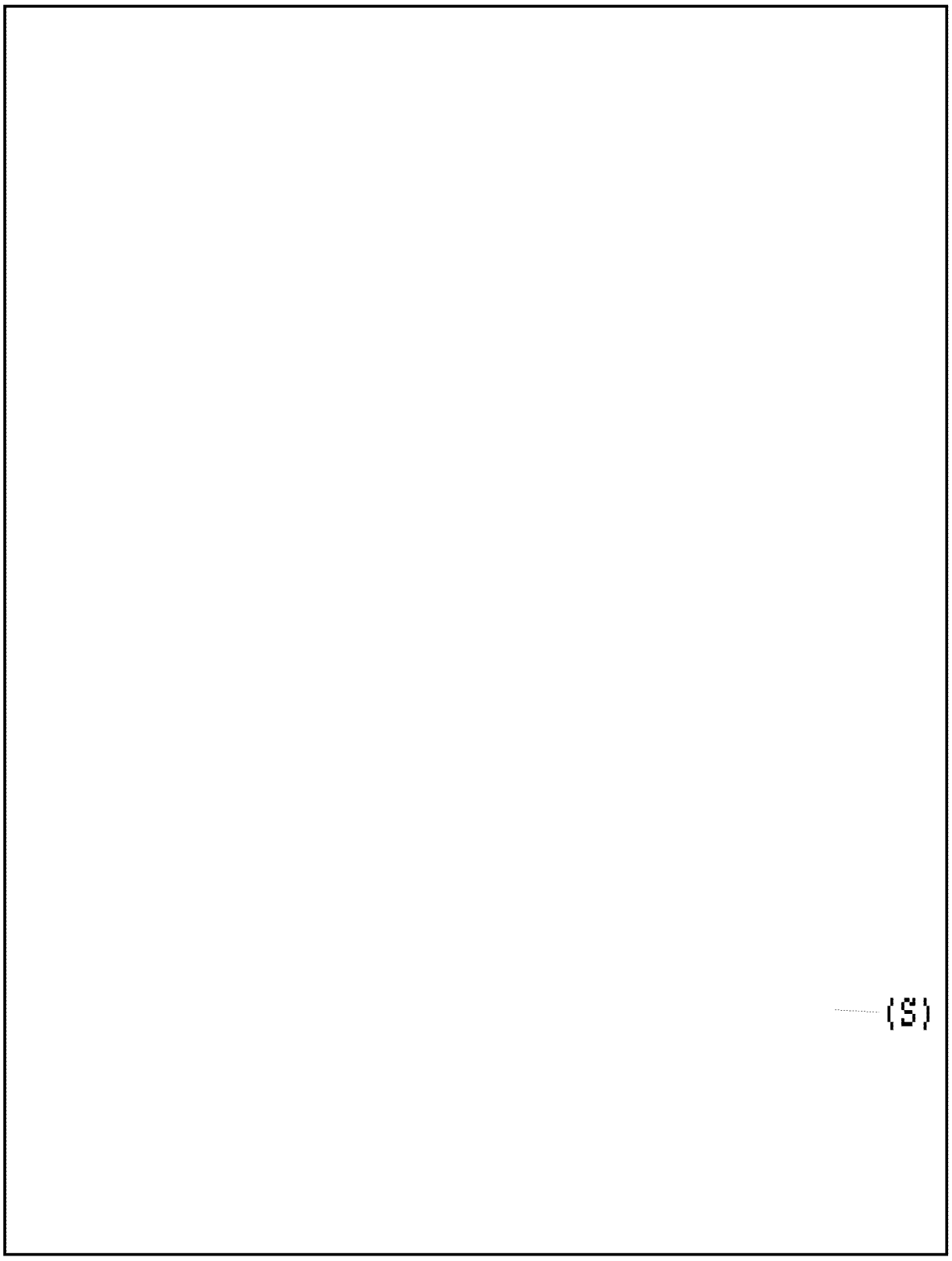
b6
b7C
b5



b5

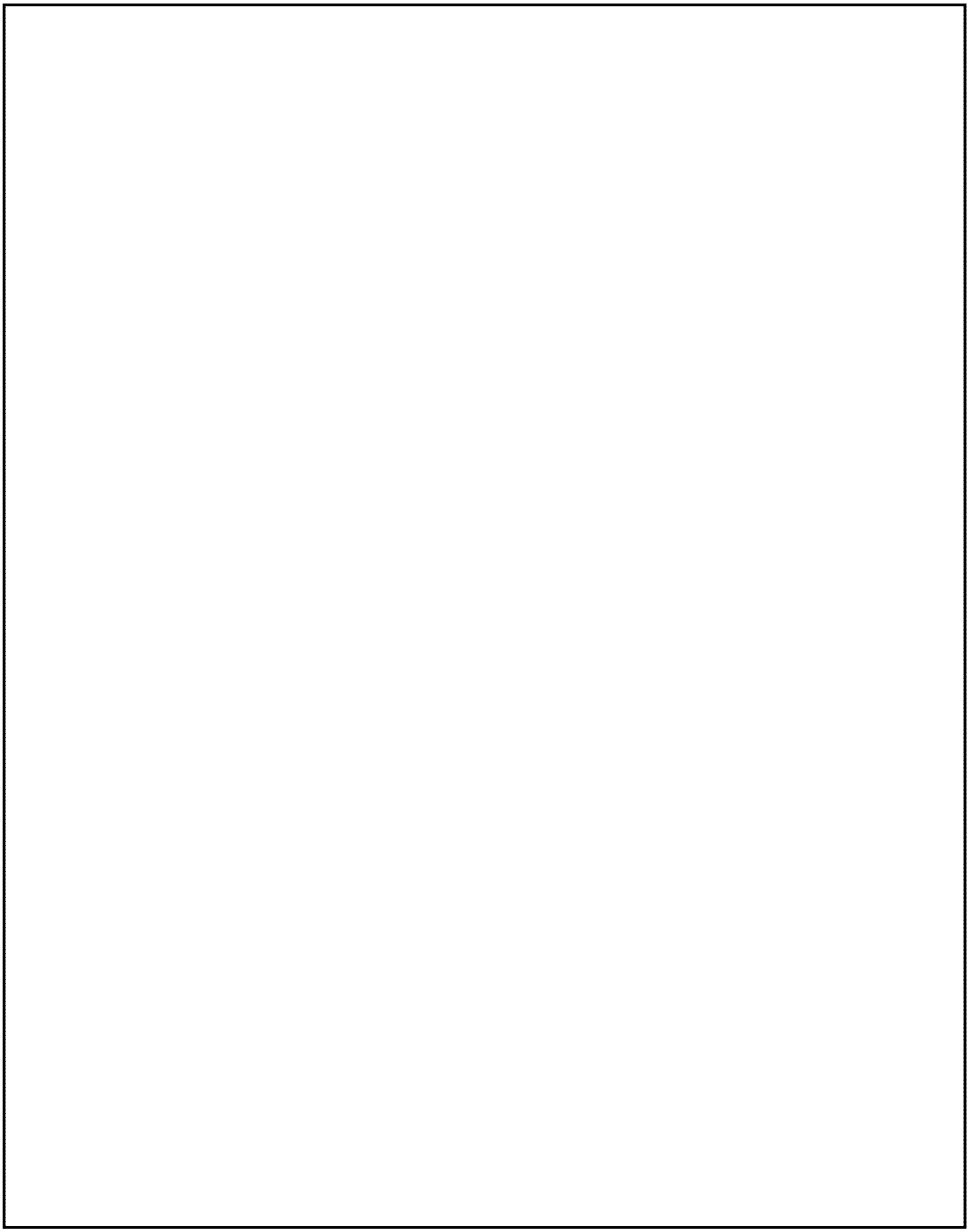


b2
b7E
b5

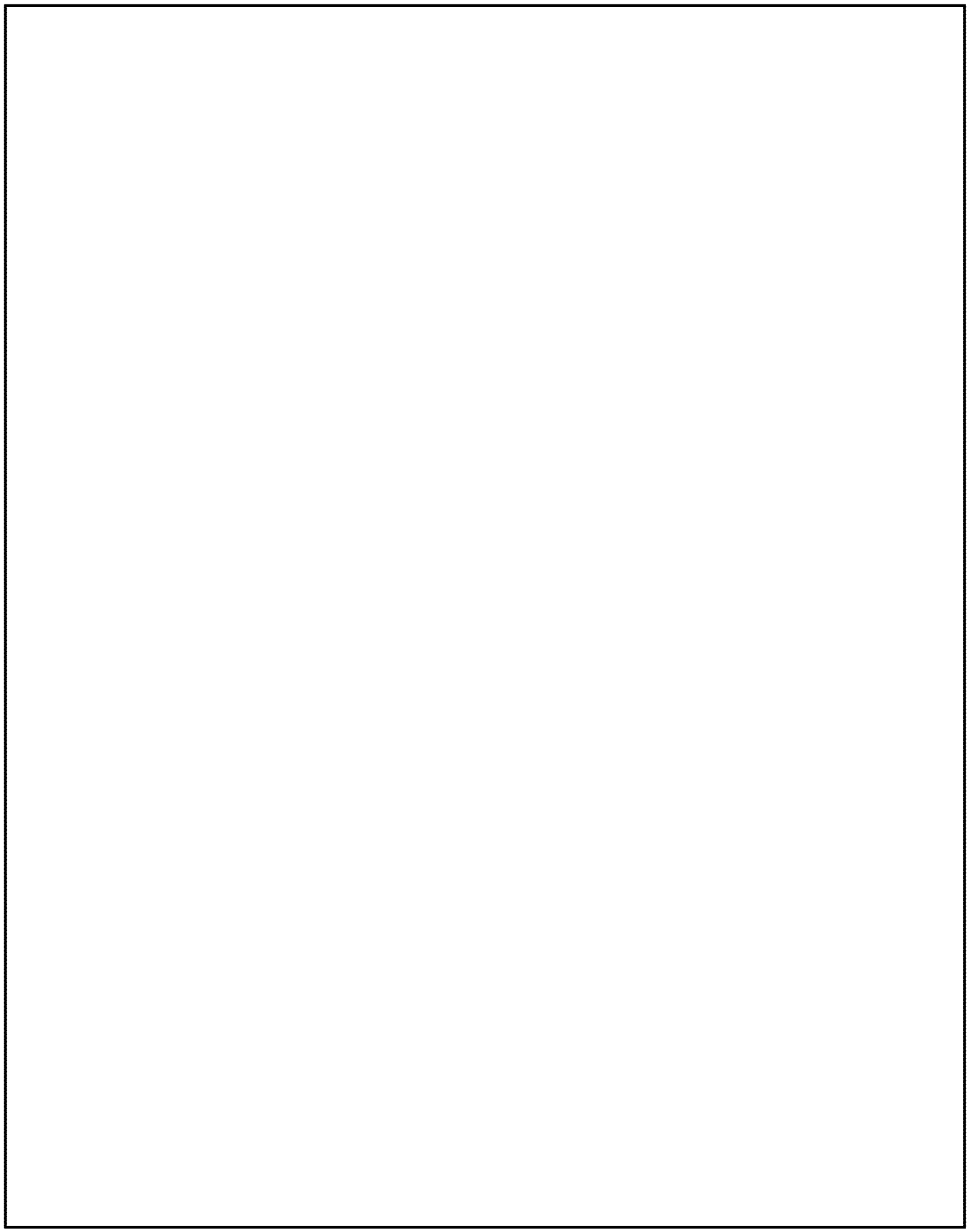


b1
b2
b7E
b5

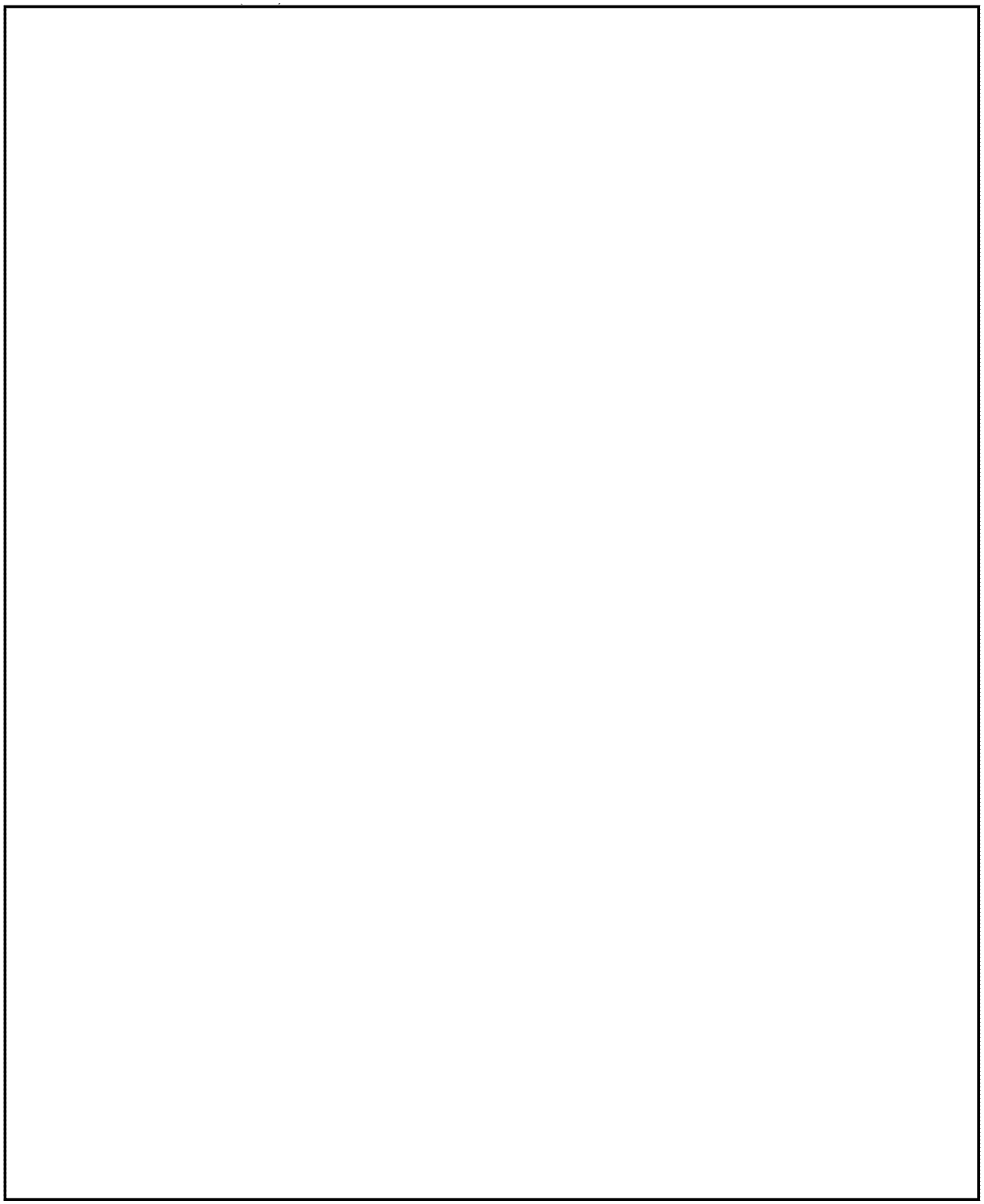
(S)



b5



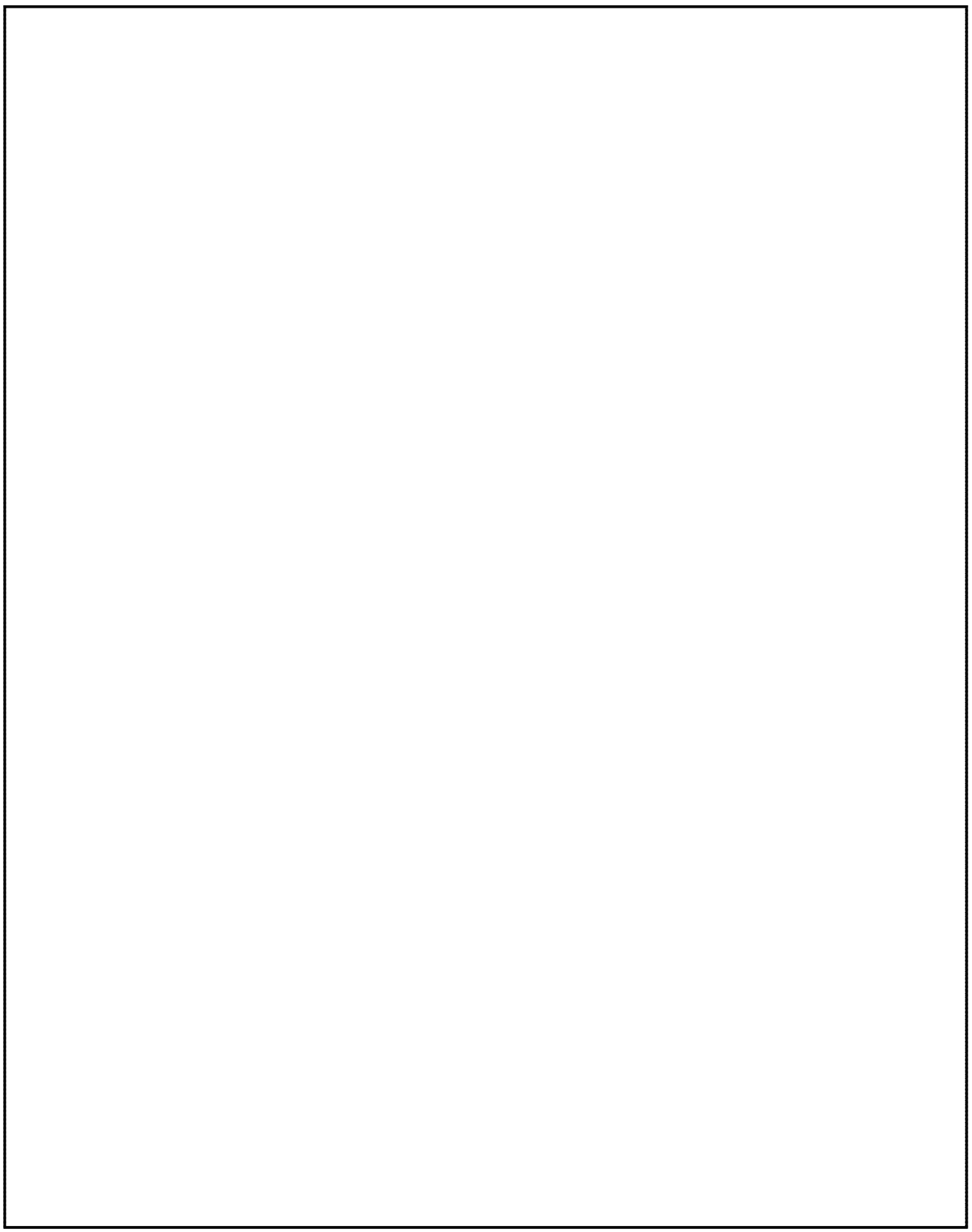
b5



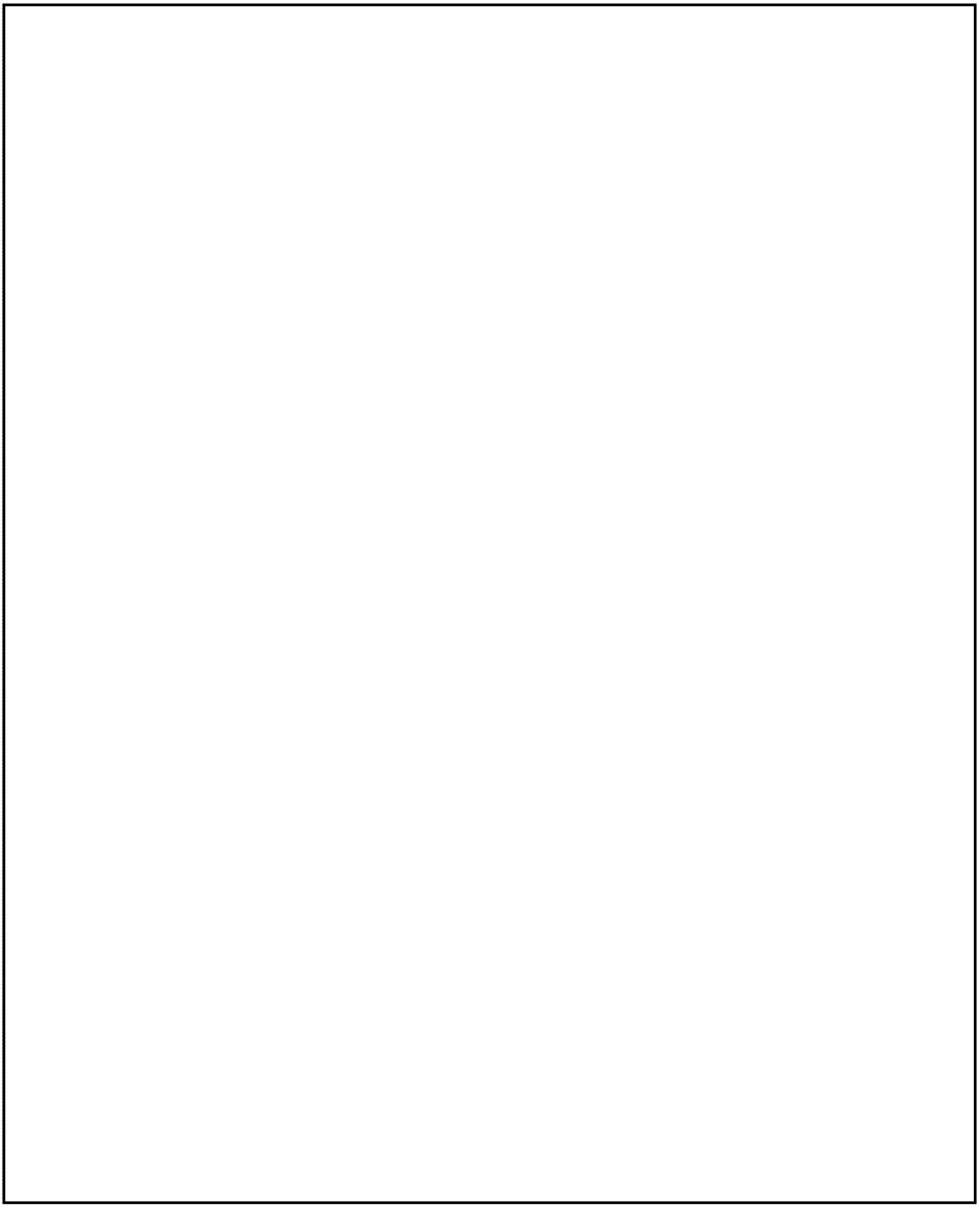
b5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

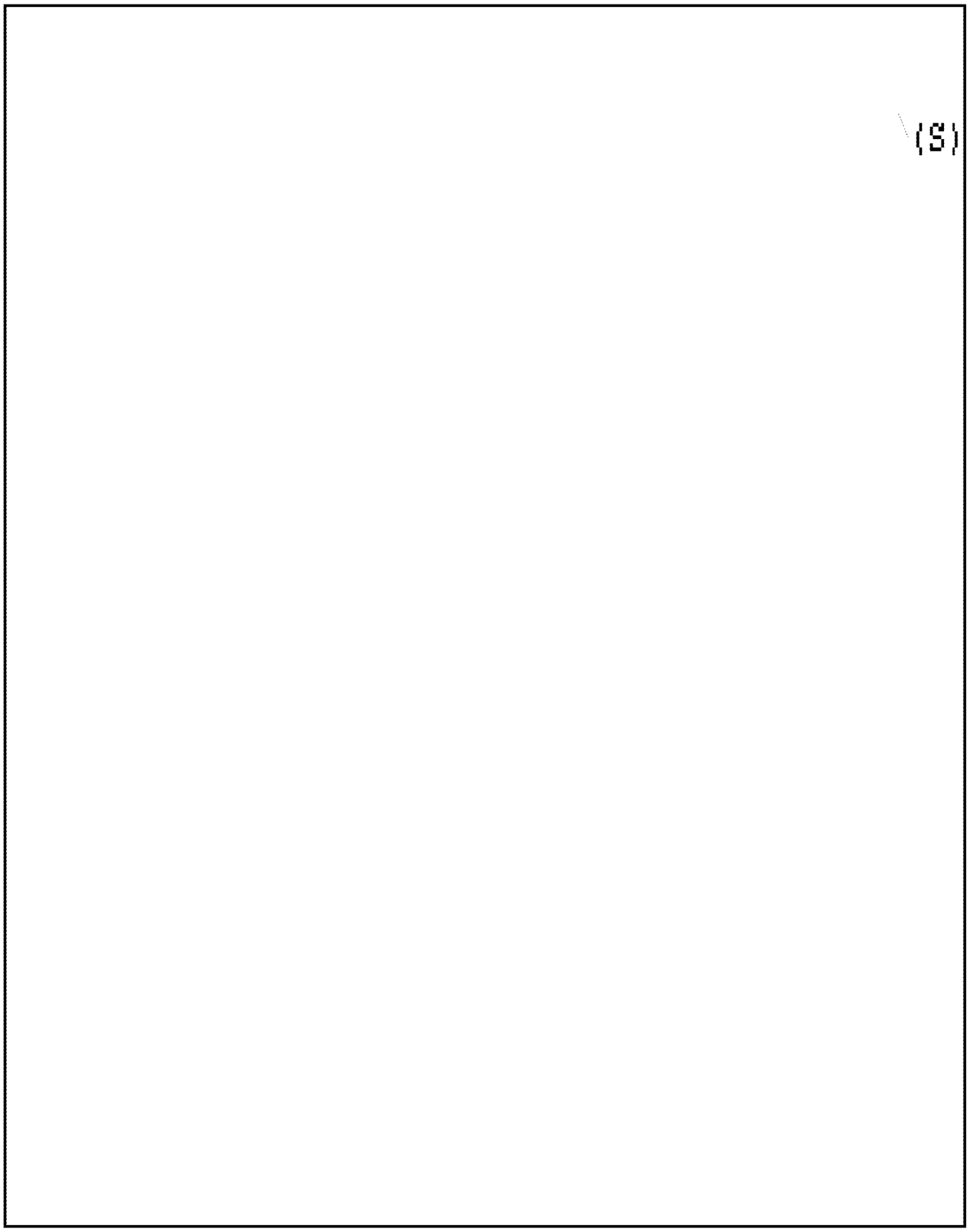
b5



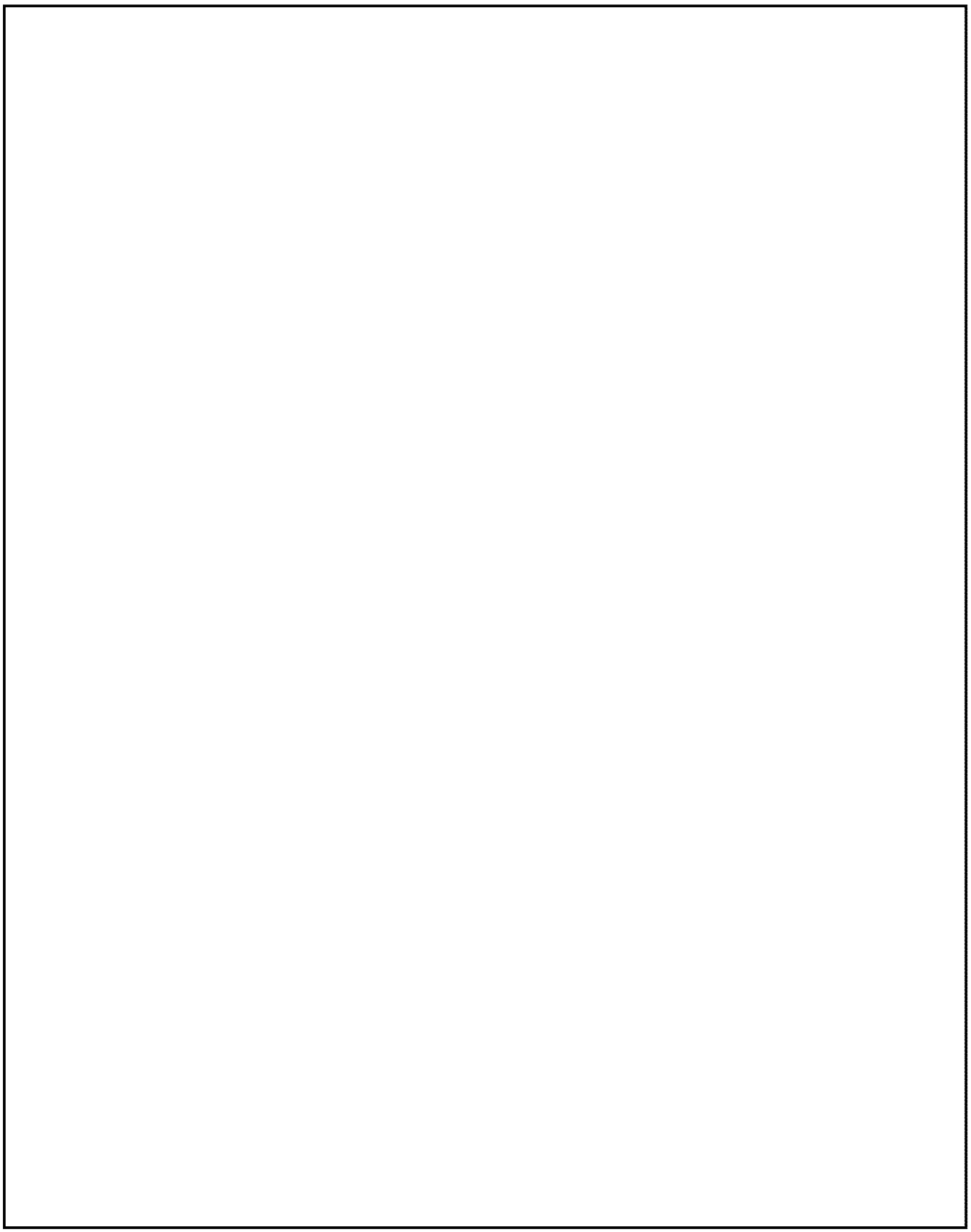
b5
b2
b7E



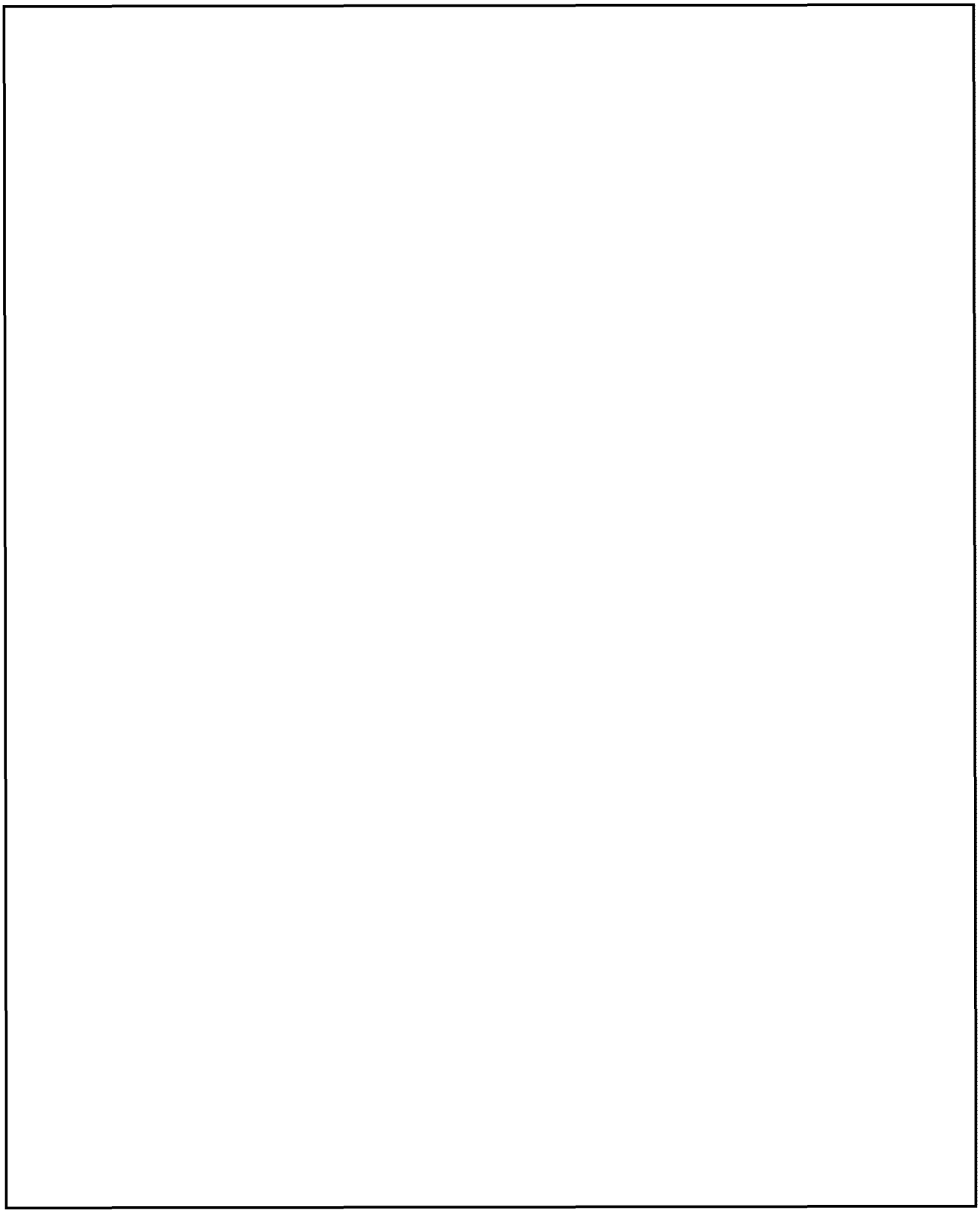
b5
b7E



b5
b2
b7E
b1



b5



b5
b2
b7E

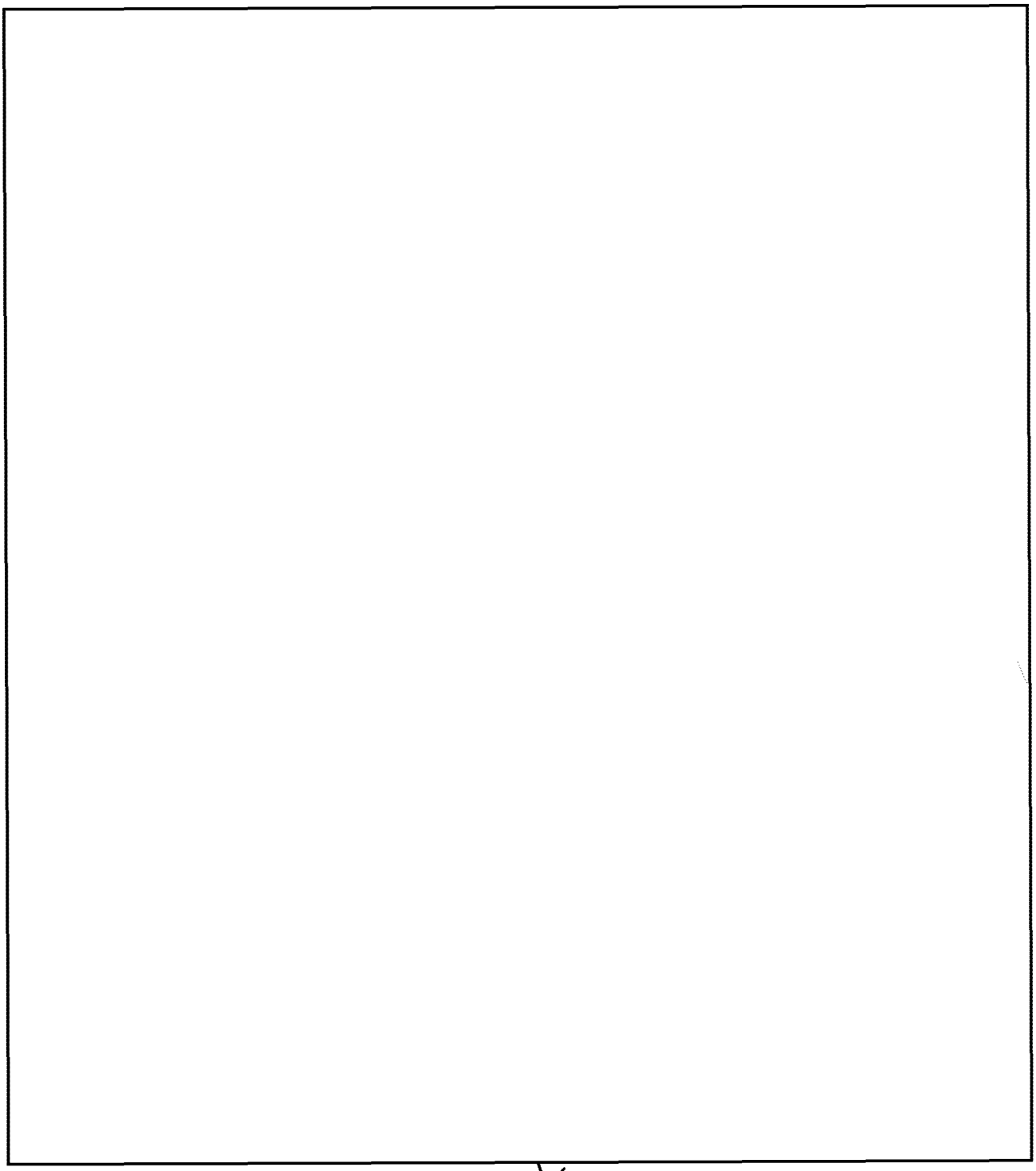
FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 62
Page 44 ~ Duplicate
Page 45 ~ Duplicate
Page 46 ~ Duplicate
Page 47 ~ Duplicate
Page 48 ~ Duplicate
Page 49 ~ Duplicate
Page 50 ~ Duplicate
Page 51 ~ Duplicate
Page 52 ~ Duplicate
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 55 ~ Duplicate
Page 56 ~ Duplicate
Page 57 ~ Duplicate
Page 58 ~ Duplicate
Page 59 ~ Duplicate
Page 60 ~ Duplicate
Page 61 ~ Duplicate
Page 62 ~ Duplicate
Page 63 ~ Duplicate
Page 64 ~ Duplicate
Page 65 ~ Duplicate
Page 66 ~ Duplicate
Page 67 ~ Duplicate
Page 68 ~ Duplicate
Page 69 ~ Duplicate
Page 70 ~ Duplicate
Page 71 ~ Duplicate
Page 72 ~ Duplicate
Page 73 ~ Duplicate
Page 74 ~ Duplicate
Page 75 ~ Duplicate
Page 76 ~ Duplicate
Page 77 ~ Duplicate
Page 78 ~ Duplicate
Page 79 ~ Duplicate
Page 80 ~ Duplicate
Page 81 ~ Duplicate
Page 82 ~ Duplicate
Page 83 ~ Duplicate
Page 84 ~ Duplicate
Page 85 ~ Duplicate
Page 86 ~ Duplicate
Page 87 ~ Duplicate

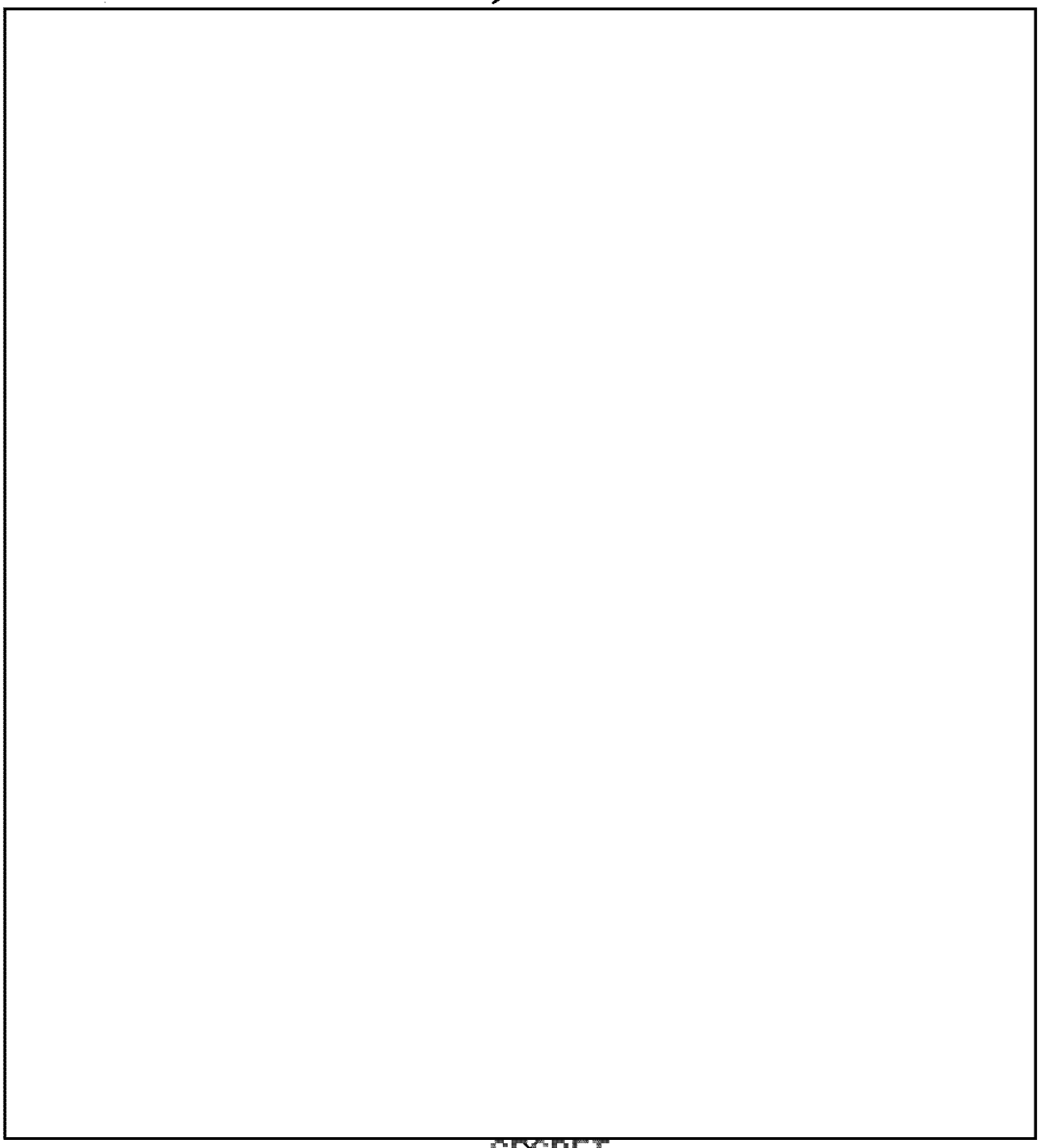
Page 88 ~ Duplicate
Page 89 ~ Duplicate
Page 90 ~ Duplicate
Page 91 ~ Duplicate
Page 92 ~ Duplicate
Page 93 ~ Duplicate
Page 94 ~ Duplicate
Page 95 ~ Duplicate
Page 96 ~ Duplicate
Page 97 ~ Duplicate
Page 98 ~ Duplicate
Page 99 ~ Duplicate
Page 100 ~ Duplicate
Page 101 ~ Duplicate
Page 102 ~ Duplicate
Page 103 ~ Duplicate
Page 104 ~ Duplicate
Page 105 ~ Duplicate

b5

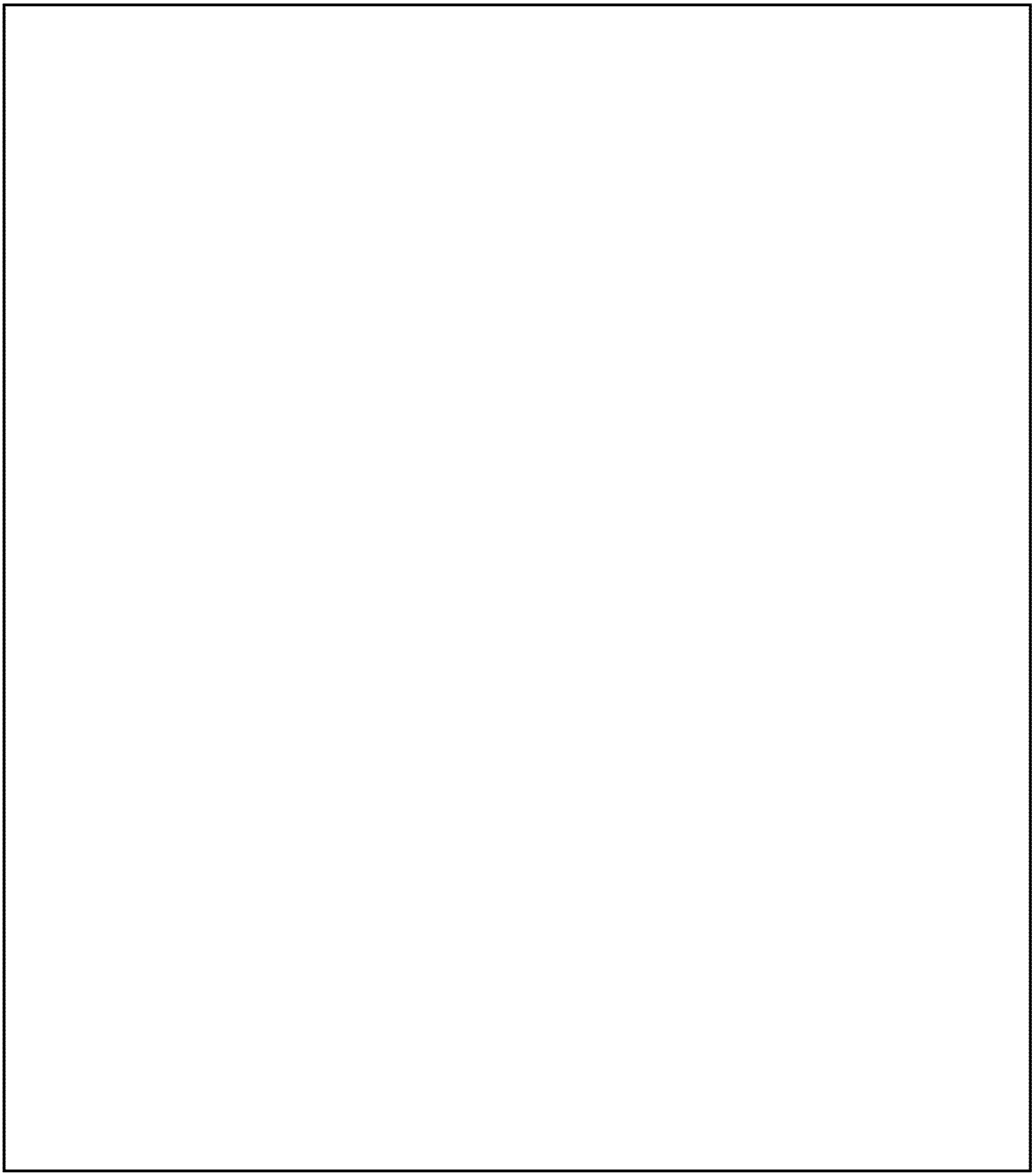


b1
b2
b5

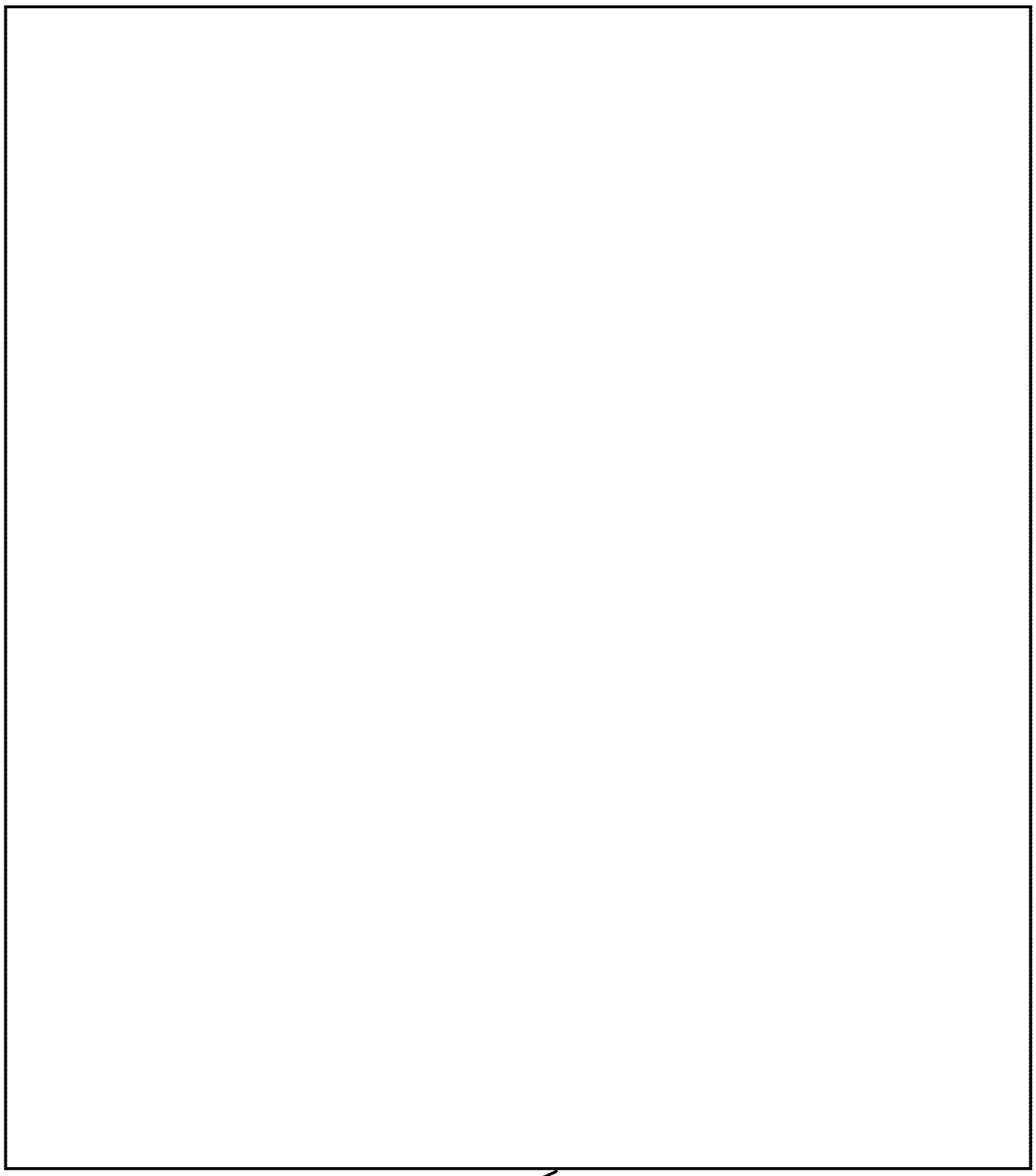
(S)



b5



b5



b5

~~SECRET~~

Responses of Robert S. Mueller, III
Director
Federal Bureau of Investigation
Based Upon July 23, 2003 Testimony
Before the Senate Committee on the Judiciary

Classification per OGA letter dated 08-17-2005

Questions Posed by Senator Hatch

As you know, I have been - and remain - concerned about the issues surrounding the death of Kenneth Michael Trentadue, an inmate who died in the Federal Transfer Center (FTC), in Oklahoma City, Oklahoma, on August 21, 1995. At approximately 3 a.m. on August 21, 1995, FTC correctional officers found Mr. Trentadue hanging by a bed sheet around his neck from a grate in his cell.

FTC officials notified the Oklahoma City FBI about Trentadue's death. I understand that a number of entities, including the FBI, the Justice Department's Civil Rights Division, the Justice Department's Inspector General's Office, the Oklahoma Medical Examiner's Office and the Oklahoma County District Attorney's Office have investigated this matter and reached a determination that Mr. Trentadue was not murdered but committed suicide. Notwithstanding the results of these investigations, I continue to have concerns as to the circumstances of Mr. Trentadue's death. To this end, I want to ask several follow up questions relating to the death of Kenneth Michael Trentadue:

1. **Please describe the FBI's involvement in the investigation of Mr. Trentadue's death, and the steps taken by the FBI during its investigation. In describing the FBI's involvement, please address all aspects of the FBI's investigation, including witness interviews, collection and processing of evidence, and all forensic examinations.**

Response:

The FBI's Oklahoma City Division was notified of Mr. Trentadue's death on August 21, 1995. The Oklahoma City Division took photographs, collected evidence, and opened an investigation into Mr. Trentadue's death. During the first few months of the investigation, the Oklahoma City Division interviewed Bureau of Prisons personnel at the Federal Transfer Facility, sent investigative leads to other field offices requesting that they locate and interview Trentadue family members and inmates who had been at the Federal Transfer Facility at the time of Mr. Trentadue's death, and sent evidence to the FBI Laboratory for forensic examination. In December 1995, the Oklahoma City Division assigned an additional Agent to the investigation in order to increase the investigative effort, and after that time additional forensic tests and numerous interviews were conducted.

Leahy 33. Finding 16 of the Joint Inquiry Report states that prior to September 11, 2001, "there was no coordinated U.S. Government-wide strategy to track terrorist funding and close down their financial support networks." Please describe the current strategy being used to track terrorist funding. What has been done since September 11th to "close down" financial support networks of terrorist activities? If the PATRIOT Act was used in any measure to "close down" a financial support network, please describe those efforts and results in detail.

Response:

Currently, there exists a much better understanding of terrorist financing methods than prior to the 9/11 attacks. More sophisticated and effective processes and mechanisms to address and target terrorist financing continue to be developed and to evolve. Pro-active approaches are increasingly being used. Awareness throughout the world on the part of law enforcement, government agencies, regulators, policy makers, and the private sector of terrorist financing methods, suspicious financial activity, and vulnerabilities is much higher since 9/11. International cooperation has reached unparalleled levels. Outreach with, and cooperation from, the private sector has been outstanding and continues to develop, particularly the level of two-way interaction between law enforcement and the private sector. The ability to access and obtain this type of information immediately has significantly enhanced the FBI's ability to identify, investigate, and resolve immediate threat situations involving potential terrorist activity. For example, the ability to monitor specifically identified financial activity has been invaluable not only to investigations ongoing in the United States, but also to foreign law enforcement and intelligence agencies in related investigations.

Extensive training and support of international investigations by the FBI's Terrorist Financing Operations Section (TFOS) has led to Agent visits, exchanges, and training programs involving a variety of countries in Europe, Southeast Asia, the Middle East, and South America. In support of specific high-profile joint terrorist financial investigations, a number of countries and agencies, including the United Kingdom, Switzerland, Canada, and Europol, have detailed investigators to TFOS on a temporary duty basis. TFOS has engaged in extensive coordination with authorities of numerous foreign governments in terrorist financing matters, leading to joint investigative efforts throughout the world. These joint investigations have successfully targeted the financing of several overseas al Qaeda cells, including those located in Indonesia, Malaysia, Singapore, Spain, and Italy. Furthermore, with the assistance of relationships established with the central banks of several strategic countries, successful disruptions of al Qaeda financing have been accomplished in countries such as the United Arab Emirates, Pakistan, Afghanistan, and Indonesia.

TFOS has developed a specific curriculum regarding terrorist financing/money laundering crimes for use in international training. This curriculum includes such topics as: acquiring and handling evidence in document intensive financial investigations, major case management techniques,

forensic examination tools, and methods of terrorist financing. At the request of DOS, TFOS has led an interagency team to provide this curriculum to a number of countries identified as needing law enforcement training on conducting terrorist financing investigations (training in approximately 38 countries is currently scheduled).

TFOS has cultivated and maintains contact with private industry and government sources/persons who can provide financial data, including real-time monitoring of financial transactions. Many of these contacts can be reached or accessed regarding emergencies 24 hours a day 7 days a week, allowing TFOS to respond rapidly to critical incidents.

Through these contacts, TFOS has access to data and information from a variety of entities including: banking institutions; credit/debit card services; money services businesses; securities and brokerage firms; insurance companies; travel agents; Internet service providers; the telecommunications industry; law enforcement agencies; federal and state regulatory agencies; public and open source data providers; the intelligence community; and international law enforcement and intelligence contacts. The timeliness and accessibility of the data are contingent on a variety of factors including whether the acquisition of the information requires legal process, the search capabilities of the data provider, and the size and depth of the data request. The ability to access and obtain this type of information quickly has significantly enhanced the FBI's ability to identify, investigate, and resolve immediate threat situations involving potential terrorist activity.

The ability to identify and track financial transactions and links after a terrorist act has occurred, or terrorist activity has been identified, represents only a small portion of the mission; the key lies in exploiting financial information to identify previously unknown terrorist cells, recognize potential terrorist activity/planning, and predict and prevent potential terrorist acts. Prior to 9/11, less emphasis was placed on addressing the mechanisms and systems associated with terrorist financing and disrupting them before they could be utilized to further terrorist activities. Since 9/11, TFOS, together with DOJ's Criminal Division's Counterterrorism Section, has begun a number of proactive link analysis initiatives to identify potential terrorists and terrorist related financing activities.

The overriding goal of these projects is to proactively identify potential terrorists and terrorist related individuals, entities, mechanisms, and schemes through the digital exploitation of data. To accomplish this, TFOS seeks to: 1) identify potential electronic data sources within domestic and foreign government and private industry providers; 2) create pathways and protocols to acquire and analyze the data; and 3) provide both reactive and proactive operational, predictive, and educational support to investigators and prosecutors.

Information sharing is critical to all of our efforts. The intelligence community, including the FBI, produces and obtains tremendous amounts of classified intelligence information. While much of the information can be of significant value in terrorist finance investigations, the value will not be realized or maximized absent the ability to filter the information, analyze it, and

disseminate it in an appropriate manner to those who can make the best use of the information. Toward this end, TFOS participates, among other joint activities, in joint endeavors involving the CIA, FBI, Treasury Department, DOJ, and DHS involving potential terrorist-related financial transactions. TFOS has personnel detailed to the CIA Counterterrorism Cente[redacted] b1 (S)

The NSC formalized the PCC at the end of 2001. The Department of Treasury chairs the PCC and representatives from the CIA, DOD, DOJ, DHS, NSC, DOS, and FBI attend meetings. The PCC generally meets at least once a month to coordinate the United States government's campaign against terrorist financing. The meeting generally focuses on ensuring that all relevant components of the federal government are acting in a coordinated and effective manner to combat terrorist financing.

Our efforts to combat terrorism have been greatly aided by the authorities of the USA PATRIOT Act. Success in preventing another catastrophic attack on the United States homeland would have been much more difficult, if not impossible, without the Act. It has already proved extraordinarily beneficial in the war on terrorism, and our opportunities to use it will only increase. Most importantly, the PATRIOT Act has produced greater collection and sharing of information within the law enforcement and intelligence communities.

Title III of the Act, known as the International Money Laundering Anti-Terrorist Financing Act of 2001, has armed us with a number of new weapons in our efforts to identify and track the financial structure supporting terrorist groups. Past terrorist financing methods have included the use of informal systems for transferring value in a manner that is difficult to detect and trace. The effectiveness of such methods should be significantly eroded by the Act, which establishes stricter rules for correspondent bank accounts, requires securities brokers and dealers to file Suspicious Activity Reports (SARs), and mandates that certain money services register with FinCEN and file SARs for a wider range of financial transactions.

Other provisions of the Act have considerably aided our efforts to address the terrorist threat including: strengthening the existing ban on providing material support to terrorists and terrorist organizations; the authority to seize terrorist assets; and the ability to seize money subject to forfeiture in a foreign bank account by authorizing seizure of a foreign bank's funds held in a United States correspondent account.

Leahy 34. **In your July 22, 2003 response to questions posed by Senator Cantwell following our June 6, 2002 hearing, regarding concerns that new authorities under the PATRIOT Act will be abused by the FBI (Question 6), you stated, "The FBI has a number of internal and external safeguards in place today that did not exist in the past." You then cited as "two key external safeguards" Executive Order 12333 - which was signed by President Reagan in 1981 -- and the FCIG - which was put in place by Attorney General Reno**

in 1995. You also cited as an "important internal safeguard" the Intelligence Oversight Board established by Executive Order 12863 - which President Clinton issued in 1993.

A. On what basis did you state that these "internal and external safeguards" are "in place today" but "did not exist in the past?"

Response:

The safeguards referenced in the question, Executive Order 12333 and the FCIG, were cited in response to a question that asked, "What assurances can you give us that these new authorities will not be abused in the name of terrorism or intelligence matters, as similar authorities had been abused by the FBI in the past?" We believed that the question's mention of "past abuses" referred to the sort of activities exposed in the 1976 report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, better known as the "Church Committee." Executive Order 12333 and the FCIG did not exist during that era, but are in place now. We did not mean to suggest that these safeguards were not in existence when the USA PATRIOT Act was passed.

B. Can you identify any safeguards against FBI abuse of its PATRIOT Act and other investigative authorities that are now in place, but did not exist prior to September 11, 2001?

Response:

There are formal and informal safeguards against FBI abuse of its investigative authorities that did not exist prior to September 11, 2001. First, some of the investigative authorities that were created or expanded by the USA PATRIOT Act contain safeguards against abuse. For example, Section 214 of the Act altered the standards for obtaining a pen register under FISA. Such a pen register may be obtained upon a certification that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities. Section 214 also now requires that the pen register applicant certify to the court that the underlying investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment. Such a certification requirement ensures that individuals will not be investigated solely because of what they say or how they worship. Section 214 also preserved the existing court-order requirement. Now, as before, law enforcement cannot install a pen register unless it applies for and receives permission from the FISA court.

Likewise, Section 216 (which codified the applicability of the criminal pen register/trap and trace investigative authority to Internet communications) contains a number of safeguards and restrictions. Section 216 preserved all of the law's pre-existing standards. As before, law enforcement officials must obtain court approval before installing a pen register and must show

that the information sought is relevant to an ongoing investigation. The pen/trap statute (18 U.S.C. chapter 206) was amended throughout to make clear that the contents of communications may not be the intended object of a pen register or trap and trace order. Also, in response to concerns about the FBI's investigative tool DCS1000 (formerly known as Carnivore), the USA PATRIOT Act imposed stringent reporting requirements on the government's installation of government-owned pen/trap devices on public providers' packet-switched data networks. (See 18 U.S.C. section 3123(a)(3).)

In addition, since the USA PATRIOT Act was passed, FBI agents have received guidance concerning appropriate implementation of certain provisions of the Act. This guidance will serve as a safeguard against FBI abuse of its PATRIOT Act and other investigative authorities. For example, Section 203 of the Act permitted law enforcement to share with the intelligence community information obtained from grand juries and Title III wiretaps. Pursuant to the Act, on September 23, 2002, the Attorney General issued Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons. These Guidelines require labeling of information that identifies United States persons so that it will be properly retained and disseminated by intelligence agencies.

Congressional oversight of the FBI's activities also provides some assurance that the FBI is conducting investigations in accordance with the Constitution and other law. Some of the investigative authorities modified by the USA PATRIOT Act contain safeguards in the form of requirements to report to Congress on use of these new authorities. For example, Section 215 of the Act amended the statute granting access to business records for foreign intelligence and international terrorism investigations, codified at 50 U.S.C. section 501. Pursuant to 50 U.S.C. section 502, on a semiannual basis, the Attorney General must fully inform the IC concerning all requests for production and must also provide the Committees on the Judiciary a report on the numbers of requests and orders.

In at least one instance, a law passed after the USA PATRIOT Act created an additional safeguard by imposing an additional reporting requirement. The Electronic Communications Privacy Act, codified beginning at 18 U.S.C. section 2701, provides privacy protection for electronic communications, such as e-mail and associated records. It also outlines the compulsory process that law enforcement can use to obtain both the content of communications and records held by an electronic communications service provider or a remote computing service, most often an Internet Service Provider. The USA PATRIOT Act created a voluntary disclosure provision that explicitly permits, but does not require, a service provider to disclose customer records to law enforcement in emergencies involving an immediate risk of death or serious physical injury to any person. 18 U.S.C. section 2702(b)(7); 18 U.S.C. section 2702(c)(4). With the passage of the Homeland Security Act of 2002, P.L.107-296, section 225(d)(2), the FBI was required to provide information on emergency disclosures received. This information must also be reported to Congress one year after enactment of the Homeland Security Act of 2002.

From: [redacted] FBI)
To: [redacted] FBI], [redacted]
Date: Mon, Apr 12, 2004 1:38 PM
Subject: Search and arrest of [redacted] on [redacted]

b6
b7C
b6
b7A
b7C

UNCLASSIFIED
NON-RECORD

On [redacted] at approx. 7:30 a.m., we executed a search warrant for the residence of [redacted]

[redacted]

b6
b7A
b7C

[redacted]

b7A

An arrest warrant for [redacted] was prepared based upon [redacted]

[redacted]

b6
b7A
b7C

[redacted] father [redacted] came to the residence at about 8:15 a.m. and had his attorney, [redacted] represented [redacted] was allowed to leave the scene with his father later in the morning. [redacted] father and attorney voluntarily brought [redacted] to the District Court for the 2:30 p.m. initial appearance on [redacted] The arrest warrant was issued for [redacted]

[redacted]

b6
b7A
b7C

[redacted] was taken to the FDC in [redacted] and will be held there until his detention hearing on [redacted] at 3:00 p.m.

The search went off without a hitch and everyone did a remarkable job working as a team and helping out. SA [redacted] did an excellent job as [redacted] and SSA [redacted] did an excellent job overseeing the search. At the end of the day, approximately 75 pieces of evidence were seized, of which 70 were transported by bureau plane to the East Coast and have been take to the lab in Edgewood, Maryland. [redacted] Aunt [redacted] who lives in the house next door to the apartment over her garage where [redacted] was living, was very complementary for how courteous we were in handling the matter. [redacted] Fire Department Battalion [redacted] who assisted during the entire operation, was also complementary and told me, "what you did today was a public service to our community."

b6
b7A
b7C

UNCLASSIFIED

CC: [redacted] [FBI], [redacted]

b7C
b6

b6
b7C

[redacted] (DO) (FBI)

From: [redacted] LA) (FBI)
Sent: Thursday, September 23, 2004 2:19 PM
To: LA MAIL All Employees
Subject: Agents only: Patriot Act Reporting Requirements

UNCLASSIFIED
RECORD 197A-LA-C233355

All FBI field offices are required to track the use of the Patriot Act provisions. Many provisions of the act will expire in 2005 unless renewed by Congress. Thus, we are tracking our use of the provisions. Please reply to this email if you have used any of the provisions identified below between 07/01/04 and the present. Please provide the number of times it was effectively used and specific information regarding why the technique was helpful.

Provisions that will expire on 12/31/2005:

1. Voicemail stored by a communication provider (§§ 2510 and 2703);
2. Nationwide search warrants for email (§ 220);
3. Information sharing (between criminal and CI) (§ 203);
4. Voluntary disclosure by ISP in emergencies (§ 212);
5. Immunity from civil liability for those person giving the FBI information in compliance with a FISA order (§ 225);
6. New T-III predicate crimes (chemical weapons, terrorism, and computer fraud/abuse);
7. Roving FISA surveillance (§ 206);
8. New standard for FISA pen/trap - relevancy (§ 214);
9. New standard for business records (§ 215);
10. New primary purpose for FISA - where FISA is only "a significant purpose" (§ 218); and
11. Monitoring communications of computer trespassers with victim consent (§ 217).

UNCLASSIFIED

U.S. House of Representatives
Committee on the Judiciary
F. James Sensenbrenner, Jr., Chairman

http://www.house.gov/judiciary
News Advisory
May 20, 2003
For immediate release

Contact:
Jeff Lungren/Terry Shawn - 202-225-2492
Dena Graziano 202-226-6888

Sensenbrenner/Conyers Release Justice Department Oversight Answers Regarding USA PATRIOT Act and War on Terrorism

WASHINGTON, D.C. – House Judiciary Committee Chairman F. James Sensenbrenner, Jr. (R-Wis.) and Ranking Member John Conyers, Jr. (D-Mich.) today released the answers (**http://www.house.gov/judiciary/patriotlet051303.pdf**) received last week from the Justice Department regarding the USA PATRIOT Act and the war on terrorism. Chairman Sensenbrenner and Rep. Conyers wrote Attorney General John Ashcroft on April 1, 2003 (**http://www.house.gov/judiciary/patriot040103.htm**) requesting information on these issues.

Chairman Sensenbrenner said, "The Justice Department should be commended for the timing and thoroughness of these answers. These answers will assist the Judiciary Committee in fulfilling its legislative and oversight responsibilities and should prove helpful in any future debate about extending all or part of the USA PATRIOT Act. In addition, I hope Members and the public will review the Department's answers for an accurate understanding of what the USA PATRIOT Act authorizes, and how this law is being implemented."

Ranking Member Conyers said, "I appreciate the fact that the Justice Department responded to our queries in a timely basis. I wish they would have been more forth coming in terms of manner in which and how freely the new powers have been used. I look forward to engaging in further oversight with the Department on this critical civil liberties issue."

This Justice Department stated the following in its response:

> ~Congress did not authorize a new innovation with section 215 (production of tangible records including books, records, papers, documents, etc.). Grand juries investigating ordinary crimes traditionally have the power to issue subpoenas to all manner of businesses, including libraries and bookstores. For example, federal grand juries subpoenaed records from numerous libraries during the Unabomber investigation.
>
> ~Section 215 of the USA PATRIOT Act imposes more restrictions on its use than a federal grand jury subpoena for the same records. First, a court must explicitly authorize the use of section 215 to obtain business records. Second, section 215 contains explicit safeguards for activities protected by the First Amendment, unlike federal grand jury subpoenas. Third, section 215 requires, for an investigation relating to a U.S. person, that the information be sought in an investigation to protect against international terrorism or clandestine intelligence activities.

~There has been no challenge to the propriety or legality of National Security Letters.

~There have been no administrative disciplinary proceedings or civil actions initiated under section 223 of the Act for unauthorized disclosures of intercepts.

~The Department of Justice has requested a judicial order delaying notice of the execution of a warrant under section 213 forty-seven times, and the courts have granted every request.

~ government has asked a court to find reasonable necessity for a seizure in connection with delayed notification under this section fifteen times, and the courts have granted fourteen of the requests.

~The court once has rejected the government's argument that a seizure was reasonably necessary. The court authorized the warrant but did not authorize seizure because it believed that photographs of relevant items in the storage unit would be sufficient.

~The most common period of a delay of notification of a warrant authorized by courts is seven days. Courts have authorized specific delays of notification as short as one day and as long as ninety days; other courts have permitted delays of unspecified duration lasting until the indictment was unsealed.

~The government has sought an extension of the period of delayed notice 248 times. This number includes multiple extensions for a single warrant.

~A court has never rejected the government's request for delayed notification on the ground that the period for giving delayed notice was unreasonable.

~The Department cites the recent indictment of Sami Al-Arian and other alleged members of a Palestinian Islamic Jihad (PIJ) cell in Tampa, Florida, as a case that benefitted from the Act's new standard of "a significant purpose" rather than "the purpose." The USA-PATRIOT Act was critical to the Department's ability to safeguard the Nation's security by bringing criminal charges against Al-Arian and others in February 2002.

~From the enactment of FISA in 1978 through September 11, 2001, available records indicate that Attorneys General issued 47 emergency authorizations for electronic surveillance and/or physical searches under FISA. Between September 11, 2001 and September 19, 2002, the Attorney General made 113 emergency authorizations for electronic surveillance and/or physical searches under FISA.

~The FBI has hired 264 new translators to support counterterrorism efforts, including 121 Arabic and 25 Farsi speakers.

~Section 212 (which allows computer-service providers to disclose communications and records of communications to protect life and limb) has been used to disclose vital information to law enforcement on many occasions, including one case where such records enabled agents to trace kidnappers' communications. This provision also proved invaluable in the investigation of a bomb threat against a school. An anonymous person, claiming to be a student at a high school, posted on an Internet message board a bomb death threat that specifically named a faculty member and several students. The owner and operator of the Internet message board turned over evidence that led to the timely arrest of the individual

responsible for the bomb threat. Faced with this evidence, the suspect confessed to making the threats.

~Section 216 was employed in the investigation of the murder of journalist Daniel Pearl to obtain information that proved critical to identifying some of the perpetrators.

~The Government's success in preventing another catastrophic attack on the American homeland in the 20 months since September 11, 2001, would have been much more difficult, if not impossibly so, without the USA PATRIOT Act. The Department's overall experience is that the authorities Congress provided in the Act have substantially enhanced our ability to prevent, investigate, and prosecute acts of terrorism.

~An informal survey of 45 FBI field offices reveal that fewer than ten of those offices have conducted investigative activities at mosques since September 11, 2001.

~The Department does not maintain centralized statistics on how many times agents attend public meetings.

~Every single person detained as a material witness as part of the September 11 investigation has been represented by counsel.

~Every single person detained as a material witness as part of the September 11 investigations was found by a federal judge to have information material to the grand jury's investigation.

~Each of the detained material witnesses is free to identify himself publicly.

~As of January 2003, the total number of material witnesses detained in the course of the September 11 investigation was fewer than 50.

~Approximately 90% of these material witnesses were detained for 90 days or less.

~The Attorney General has ordered the monitoring of attorney communications for a single inmate: Sheik Omar Ahmad Rahman, who was convicted for his part in the 1993 plot to bomb the World Trade Center. Rahman and his attorney were notified that their communications were subject to monitoring. No monitoring has occurred, however, because the inmate and his attorneys thus far have chose not to communicate further with each other.

The following additional information was indicated in the Department's response:

~The Department has used the new powers of the PATRIOT Act for non-terrorism cases (drug violations, credit card fraud, theft from a bank account, a lawyer who defrauded his clients).

~The Department has sought and the courts have authorized delayed notification of search warrants 47 times. Some courts have authorized delayed notification lasting until the indictment was unsealed. The Department has sought extensions of such delayed notifications 248 times.

~The Attorney General made emergency authorizations 113 times for FISA electronic

surveillance and/or physical searches in a one-year period.

~A December 24, 2002 memorandum from the Deputy Attorney General and the FBI Director providing guidance on the use of FISA to US Attorneys and all FBI agents says that FISA can be used as long as there is a significant "non-prosecutorial" purpose.

~Prior to moving to DHS, the INS did not charge any aliens with the expanded terrorism grounds of inadmissibility or deportability provided under section 411 of the PATRIOT Act.

b6
b7C

From:
Sent: Monday, August 04, 2003 11:38 AM
To:

Subject: FW: New Executive Order Re Information Sharing

FYI. I filed the Exec Ord. in elec lib

b6
b7C

-----Original Message-----
From:
Sent: Monday, August 04, 2003 11:35 AM
To:

Subject: FW: New Executive Order Re Information Sharing

b6
b7C

b6
b7C

-----Original Message-----
From:
Sent: Monday, August 04, 2003 11:28 AM
To:

Cc:
Subject: New Executive Order Re Information Sharing

Hi everyone,

Attached is a new Executive Order 13311, titled, **"Homeland Security Information Sharing,"** dated July 29, 2003. Section 892 of the Homeland Security Act, which is referred to in this EO,

specifically concerns Facilitating Homeland Security Information Sharing Procedures http://30.100.99.18/ogc/library/Homeland/home.pdf

I have also attached a law review article titled, "THE USA PATRIOT ACT'S APPLICATION TO LIBRARY RECORDS." Unsurprisingly, the law student who wrote this article comes down against the Government and our authority to search library patron records under the PATRIOT Act. *See* section 215 USA PATRIOT Act, codified at 50 USC 1861-1862 (attached).

Speaking of accessing library records, Senator Russ Feingold introduced legislation last week (The Library Bookseller and Personal Records Privacy Act) that would limit the FBI's authority to search library records, etc. . . *See attached*

Please forward to all appropriate units/squads.


EO 13311 formation sharing.w


library records PATRIOT Act.wp...


50 USC 1861.wpd (13 KB)


50 USC 1862.wpd (10 KB)


Feingold Introduces Legislatio...


getdoc.cgi_dbname =108_cong_bil...

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

From [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 4:30 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Business Records/Health Care industry

b5
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-04-2005 BY 65179 DMH/JHF 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] I don't think this is ALU turf. ILU has the turf on health records for criminal cases. So I'm sending this to [redacted] in ILU. Also to NSLB's own [redacted] recently in ILU.

-----Original Message-----
From [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 3:23 PM
To: [redacted] (OGC) (FBI)
Subject: FW: Business Records/Health Care industry

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Thanks. [redacted]

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 3:17 PM
To: BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: RE: Business Records

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] Why don't you touch base with ALU on this as well just to come up to speed on health records. Ask [redacted] who he has covering this now.

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Wednesday, October 06, 2004 11:26 AM
To: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Business Records

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, October 06, 2004 11:22 AM
To: BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: Business Records

b5
b6
b7C
b7D

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

SENSITIVE BUT UNCLASSIFIED

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

SENSITIVE BUT UNCLASSIFIED

RE RE RE FW Director's 723 Senate Hearing.txt

From:
Sent: Wednesday, July 16, 2003 12:52 PM
To:
Cc:
Rowan, J Patrick;
Subject: RE: RE: RE: FW: Director's 7/23 Senate Hearing

- here are the top picks from me and Bill. There is no particular order of importance among these:

Privacy Act:

1. Section 552a(a)(8)(B) is amended by adding the following new subsection:

"(ix) matches performed by, or at the request of, an agency (or component thereof) which performs as a principal function any activity pertaining to national security (including the prevention of terrorism), for purposes relating to national security (including the prevention of terrorism)."

2. Section 552a(e)(6) is amended by adding the following after "section": "or pursuant to a counterterrorism or national security matter."

counterterrorism and national security matters.

3. Section 552a(g) of title 5, United States Code, is amended by adding at the end the following new paragraph:

"(6) If the head of an agency exempts a system of records from this subsection as provided in subsection (j), no court shall have jurisdiction over any civil action brought against said agency for failure to comply with any provision of this Act." b5

[redacted]

4. Section 552a(j) is amended by adding the following sentence to the end of the section:

"The statement of reasons for such exemptions shall not, however, constitute a limitation on the scope of the exemptions."

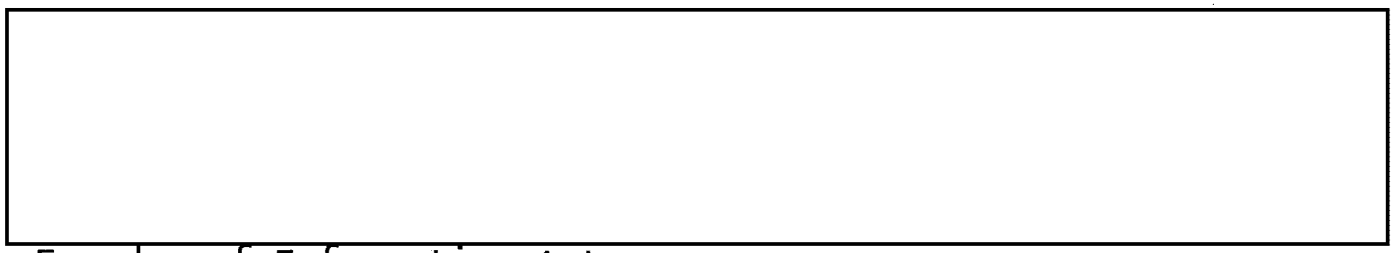
Why? This amendment is intended to reverse case law which suggests that the statement of reasons for the exemptions constitutes a limitation on the scope of the exemption. While agencies are required to publish the reasons why a system of records is to be exempted from a provision of the Act, agencies should not have to divine all possible reasons at the time of publication at the risk that such failure could be exploited by terrorists or others.

5. Section 552a(k) is amended by adding the following sentence to the end of the section:

"The statement of reasons for such exemptions shall not, however, constitute a limitation on the scope of the exemptions." b5

6. Section 552a(j)(1) is amended by striking the semi-colon and the word "Agency" and adding the following:

"or the Federal Bureau of Investigation." b5



Freedom of Information Act

1. Section 552(a)(3)(A) of title 5, United States Code, is amended by adding the following at the end:

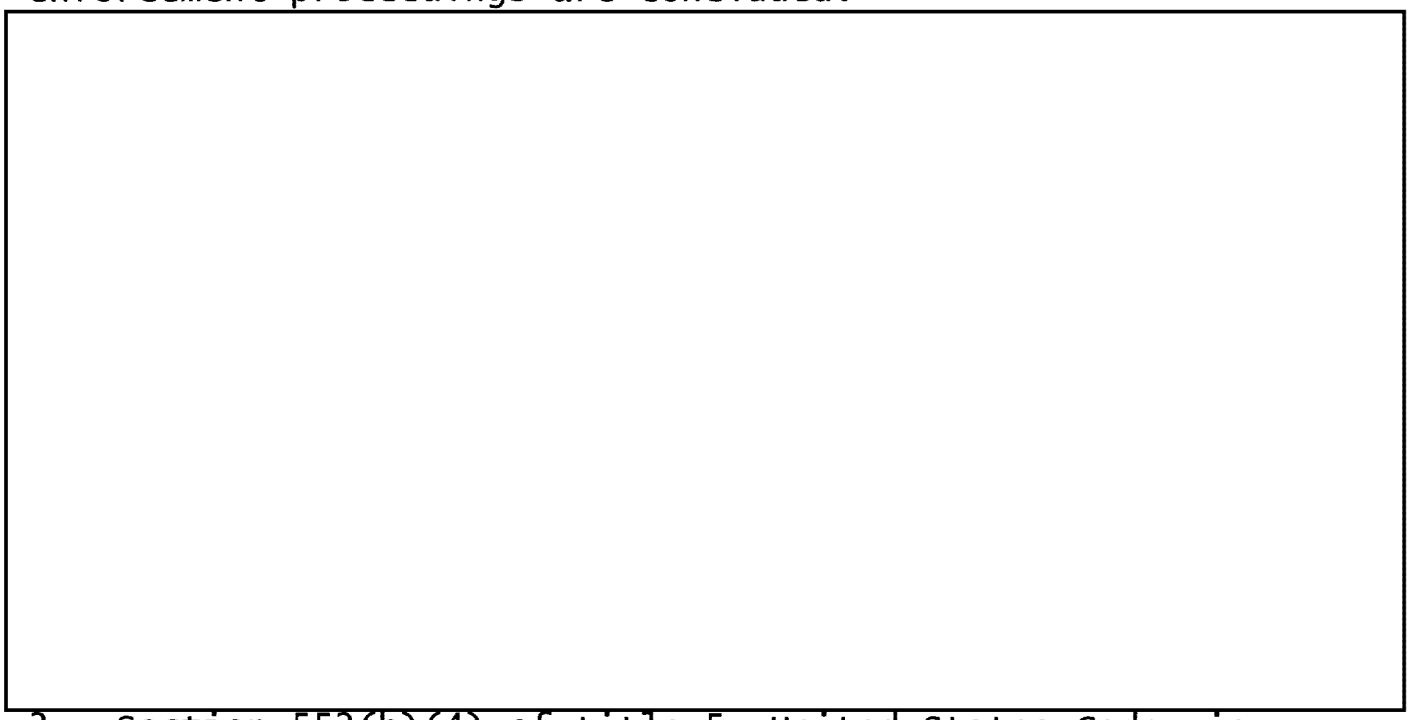
"The provisions of this paragraph shall not apply to requests submitted to agencies involved in national security, counterterrorism, homeland security or border

security matters by or on behalf of (i) foreign persons, except lawful permanent residents, or (ii) persons suspected of engaging in or supporting terrorism, foreign intelligence collection, or other activities inimical to the national security interests of the United States. As relating to records of the agencies described above, requests need not be processed, nor need any response be provided to any person, except upon a written certification of such person, subject to the penalties of 18 U.S.C. 1001, stating that person's true name and address and that the person has no knowledge or reason to belief that the request is being submitted by or on behalf of any of the persons described above. In addition to or in lieu of any criminal prosecution, the Attorney General may bring a civil action against any person who seeks or obtains records in violation of this paragraph. The court in which such action is brought may assess against such person a penalty in any amount not to exceed $100,000. Such remedy shall be in addition to any other remedy available under statutory or common law.." b5

agencies to devote limited resources to activities such as homeland security that are essential to the citizenry. This amendment will prohibit such individuals or their representatives from making FOIA requests to agencies involved in national security, counterterrorism, homeland security or border security matters. These changes will not impair due process of the persons affected because they will still retain all of the discovery rights that are otherwise available in the forum in question.

2. Section 552(b)(7) of title 5, United States Code, is amended by adding the following at the end of the last paragraph:

"An agency's claim of exemption based solely on (b)(7)(A) shall not constitute a bar to or waiver of the claim of any other exemption in this section once the enforcement proceedings are concluded." b5



3. Section 552(b)(4) of title 5, United States Code, is amended to read as follows:

"(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential. In addition, any agency may delay, for a

period not to exceed 5 years after development, the unrestricted public disclosure of technical data that could have qualified as a trade secret or commercial or financial information that is privileged or confidential if the information had been obtained from a non-Federal party, in any case in which the technical data is generated in the performance of experimental, developmental, research, counterterrorism or national security activities or programs, conducted by, or funded in whole or in part by, the agency. Such technical data referred to in this subsection shall not be subject to the disclosure requirements of this section. This paragraph shall in no way affect the applicability of any other provision of this subsection." b5

[redacted]

-----Original Message-----
From: [redacted] b6
Sent: Wednesday, July 16, 2003 9:31 AM b7C
To: [redacted]
Cc:
Subject: Re: RE: RE: FW: Director's 7/23 Senate Hearing

b5

[redacted]

RE RE RE FW Director's 723 Senate Hearing.txt

b5

Thanks for this follow up. -

b5
b6
b7C

>>> 07/16 9:14 AM >>>

-----Original Message-----
From:
Sent: Tuesday, July 15, 2003 1:51 PM
To:
Cc:
Subject: Re: RE: FW: Director's 7/23 Senate Hearing

b6
b7C

b5
b6
b7C

Thanks.

b5

[redacted]

[redacted]
Office of Congressional Affairs
Room 7252, JEH Bldg
[redacted]

b6
b7C
b2
b5
b6
b7C

>>> [redacted] 07/15 12:55 PM >>>

[redacted]

-----Original Message-----
From: [redacted]
Sent: Monday, July 14, 2003 12:23 PM
To: [redacted]
[redacted]
Cc: Steele, Charles M; [redacted]
[redacted] Kelley, Patrick W
Subject: Re: FW: Director's 7/23 Senate Hearing

b6
b7C

b5
b6
b7C

[redacted]

b2
b5
b6
b7C

RE RE RE FW Director's 723 Senate Hearing.txt

[redacted]

Thanks for playing our game!

--[redacted](ext. [redacted])

>>>[redacted]07/14 11:06 AM >>>

[redacted]

-----Original Message-----
From: [redacted]
Sent: Sunday, July 13, 2003 8:27 PM
To: Kelley, Patrick W
Cc: [redacted] Kalisch, Eleni P.; [redacted]
[redacted] Rowan, J Patrick; [redacted]
Bowman, Marion E; [redacted]
[redacted]
Subject: Director's 7/23 Senate Hearing

b5
b6
b7C
b5
b6
b7C

[redacted]

b5

b5

[redacted]

[redacted]
Office of Congressional Affairs
Room 7252, JEH Bldg

b2
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-04-2005 BY 65179 DMH/JHF 05-CV-0845

From:
Sent: Thursday, January 22, 2004 12:28 PM
To: Caproni, Valerie E.; Curran, John F.; KELLEY, PATRICK W.;
Cc:
Subject: DNA issue--change in meeting to Tuesday

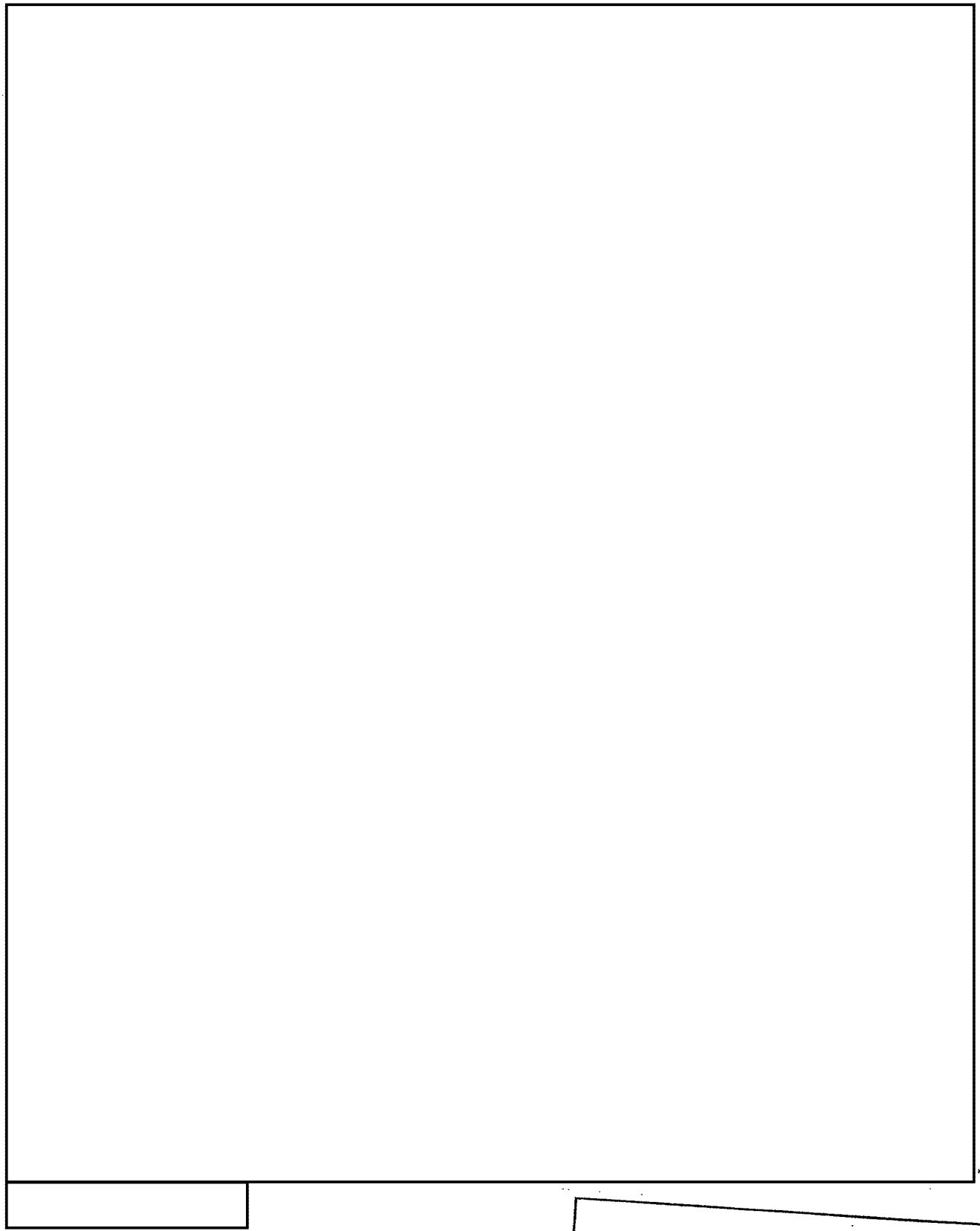
b5
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

Associate General Counsel

[redacted]rm

labafipmou.ec.w pd (31 KB)

requestfordnaby :ia2.ec.wpd (16..

b2
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 04, 2004 6:35 PM
To: [redacted] (LD) (FBI)
Cc: [redacted]
Subject: RE: sharing DNA profiles with [redacted]

b6
b7C
b7D

b5
b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] (LD) (FBI)
Sent: Tuesday, May 04, 2004 1:25 PM
To: [redacted] (Div09) (FBI)
Subject: FW: sharing DNA profiles with [redacted]

b6
b7C
b7D

UNCLASSIFIED
NON-RECORD

b6
b7C

Hi [redacted]

[redacted]

b5
b6
b7C

Thanks -
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, April 07, 2004 1:47 PM
To: [redacted] (Div09) (FBI)
Subject: sharing DNA profiles with [redacted]

b6
b7C
b7D

Expires After: 7/6/2004 00:00

Hi [redacted]

[redacted]

b5
b6
b7C
b7D

Thanks, [redacted]

UNCLASSIFIED

UNCLASSIFIED

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C

-----Original Message-----**From** [redacted] (OGC) (FBI) **Sent:** Thursday, August 19, 2004 8:47 AM**To:** [redacted] (OGC) (FBI)**Cc:** [redacted] (OGC)(FBI)**Subject:** RE: Discretionary Access Control Team

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 6:41 PM**To:** [redacted] (OGC) (FBI)**Cc:** [redacted] (OGC)(FBI)**Subject:** RE: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 5:46 PM**To:** [redacted] (OGC) (FBI)**Cc:** [redacted] (OGC)(FBI); KELLEY, PATRICK W. (OGC) (FBI); Curran, John F. (OGC) (OGA); [redacted] (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)**Subject:** RE: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 1:35 PM**To:** KELLEY, PATRICK W. (OGC) (FBI); Curran, John F. (OGC) (OGA); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)**Cc** [redacted] (OGC)(FBI)**Subject:** FW: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted] (OGC) (FBI) **Sent:** Wednesday, August 18, 2004 1:03 PM**To** [redacted] (OGC) (FBI)**Subject:** RE: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

[redacted]

-----Original Message-----**From:** [redacted](OGC) (FBI) **Sent:** Wednesday, August 18, 2004 10:29 AM**To:** [redacted](OGC) (FBI)**Cc:** Curran, John F. (OGC) (OGA); BOWMAN, MARION E. (OGC) (FBI); [redacted]OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted]OGC)(FBI); [redacted](OGC) (FBI)**Subject:** FW: Discretionary Access Control Team

b5
b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

-----Original Message-----**From:** [redacted](OI) (OGA) **Sent:** Wednesday, August 18, 2004 8:57 AM**To:** VAN DUYN, DONALD N. (CTD) (FBI); LAUGHLIN, LAURA M. (CID) (FBI); BOLLINGER, VIRGINIA L. (CD) (FBI); SEAVEY, GAIL M. (CyD) (FBI); [redacted](SecD) (OGA)[redacted](OGC) (FBI); [redacted](OI) (FBI)**Cc:** [redacted](ITOD)(FBI); [redacted](ITOD)(FBI); [redacted](CTD) (FBI); [redacted](OGC) (FBI); BERNAZZANI, JAMES (OI) (FBI); BAGINSKI, MAUREEN A. (DO) (FBI); BROCK, KEVIN R. (CI) (FBI); [redacted]DO) (FBI); AZMI, ZALMAI (OCIO) (FBI)[redacted](SecD) (FBI)**Subject:** Discretionary Access Control Team

b6
b7C

UNCLASSIFIEDNON-RECORD

[redacted]

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

[redacted]

b5
b6
b7C
b2

Thanks,

[redacted]

Office of Intelligence [redacted]

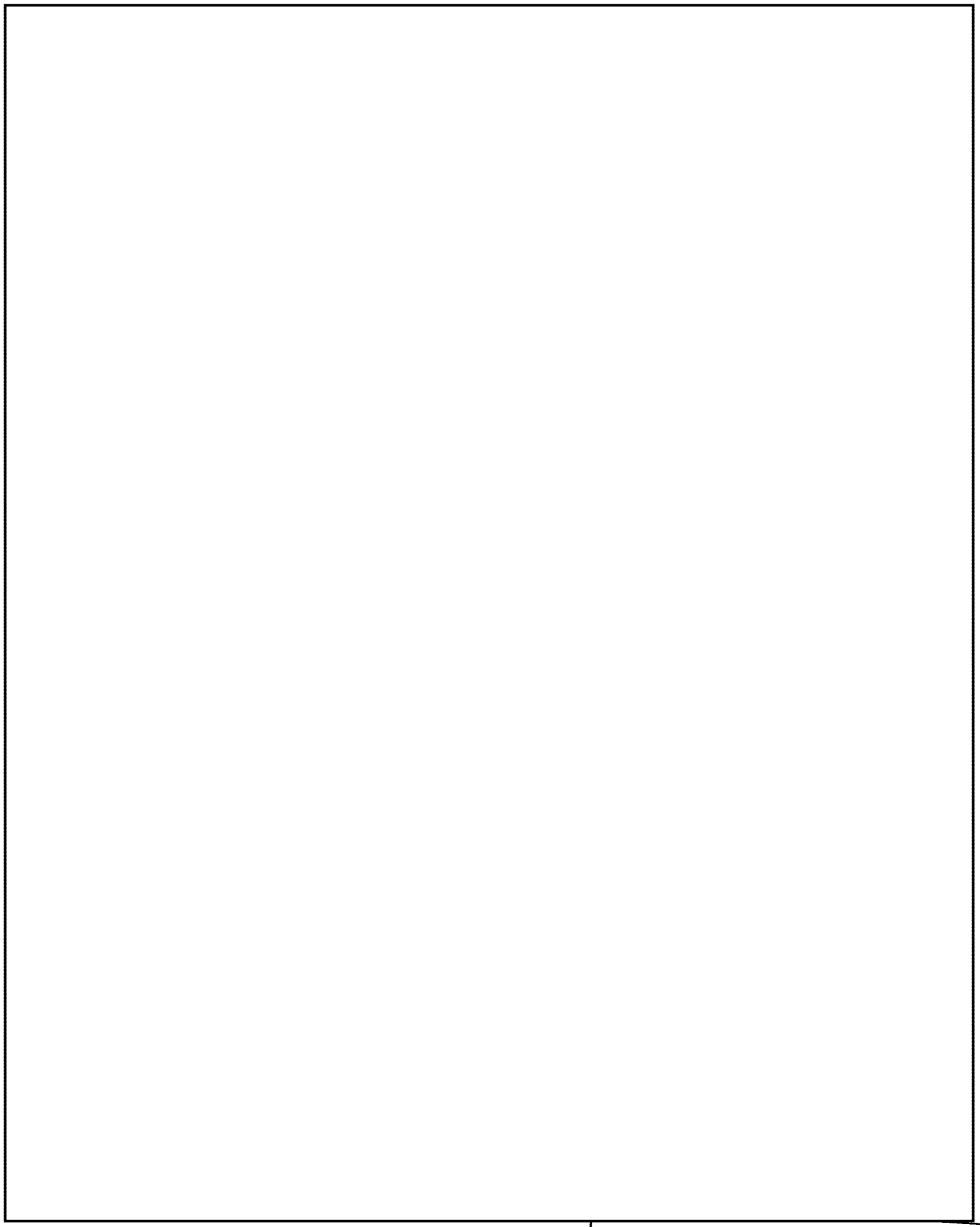
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

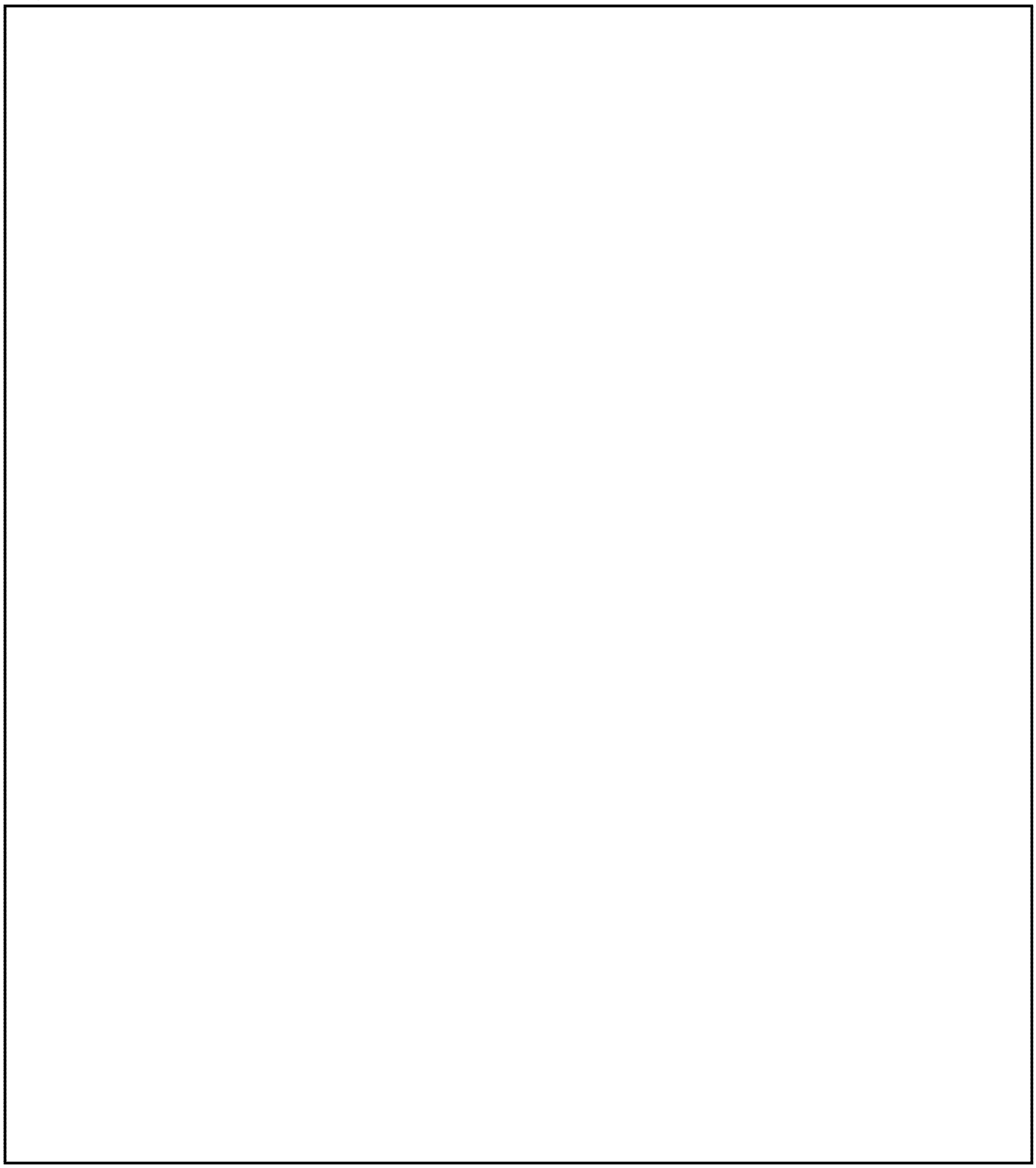
RESTRICTIONS AND CONDITIONS ON DISCLOSING FBI INFORMATION FROM INTERNATIONAL TERRORISM (315) INVESTIGATIONS TO THE NATIONAL COUNTER-TERRORISM CENTER AND OTHER COMPONENTS OF THE INTELLIGENCE COMMUNITY

b5

I. RESTRICTIONS BASED ON THE TYPE OF CRIMINAL LEGAL PROCESS

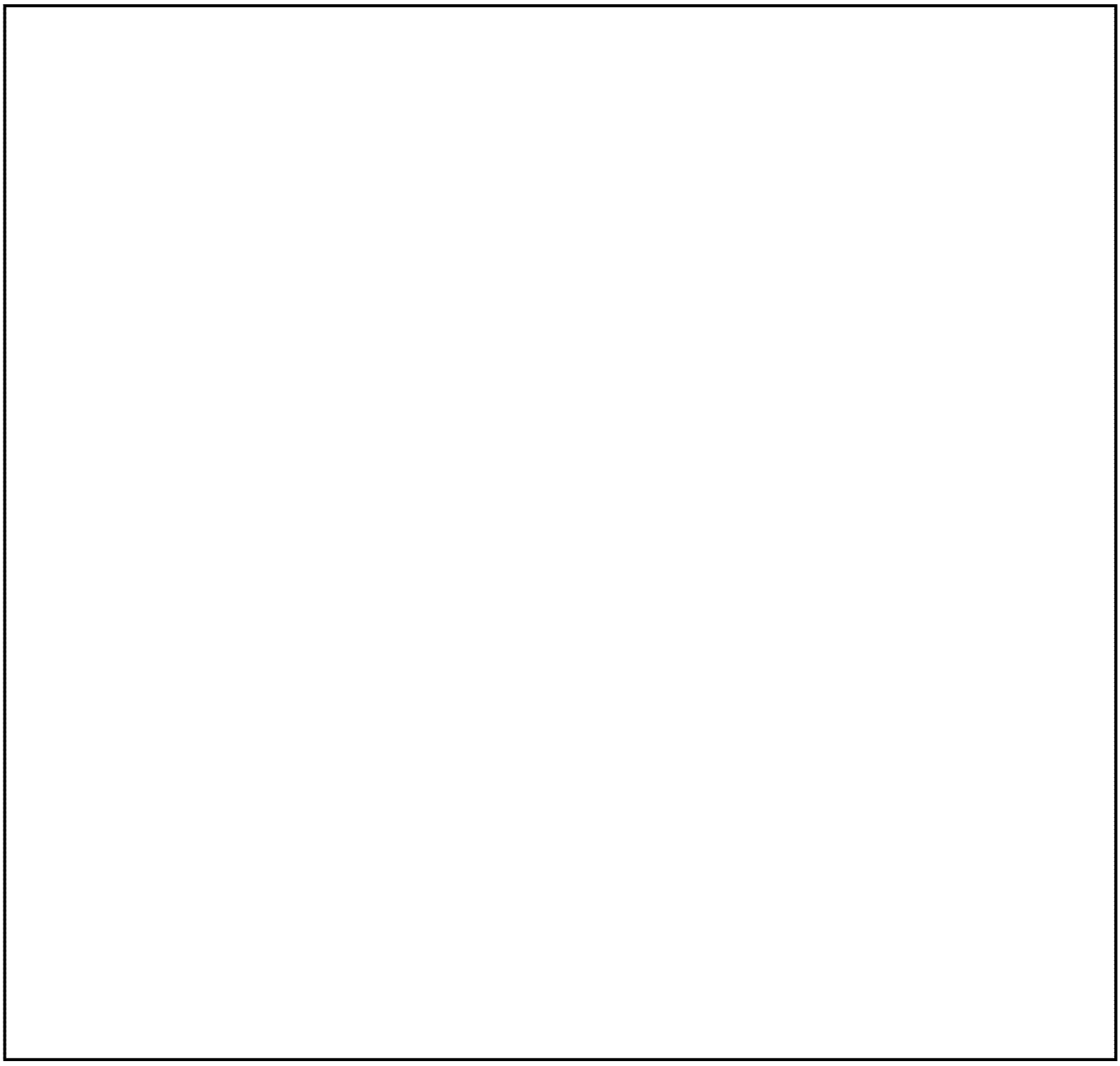
b5



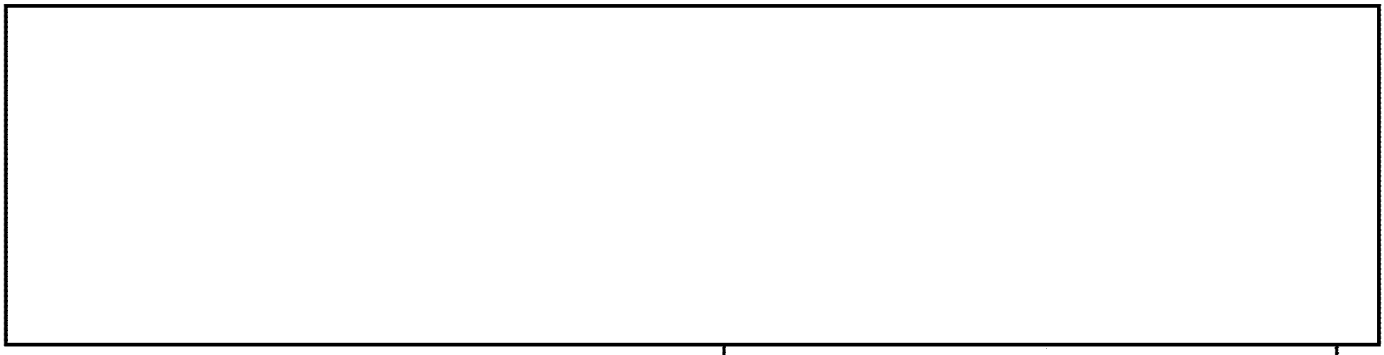


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

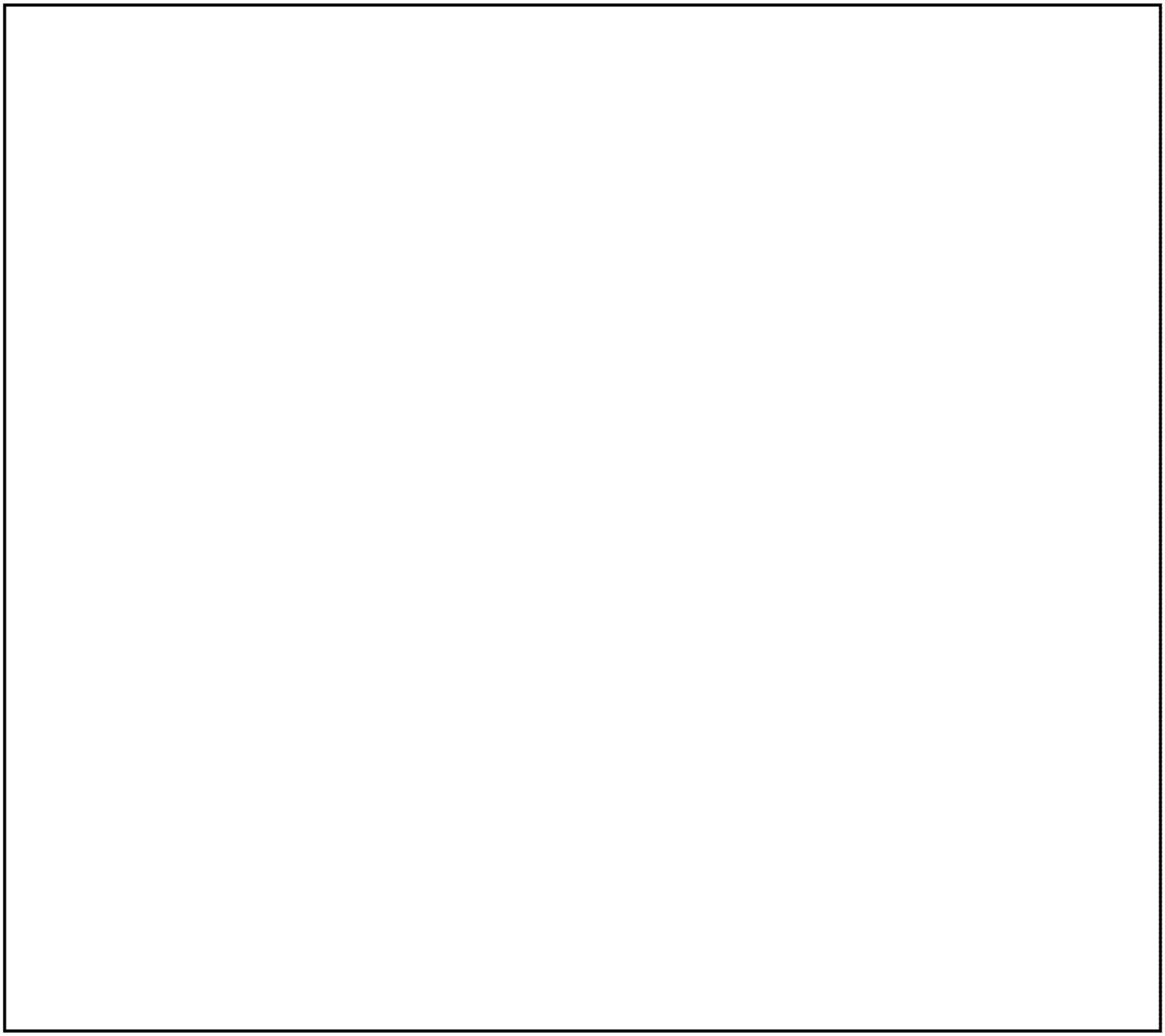


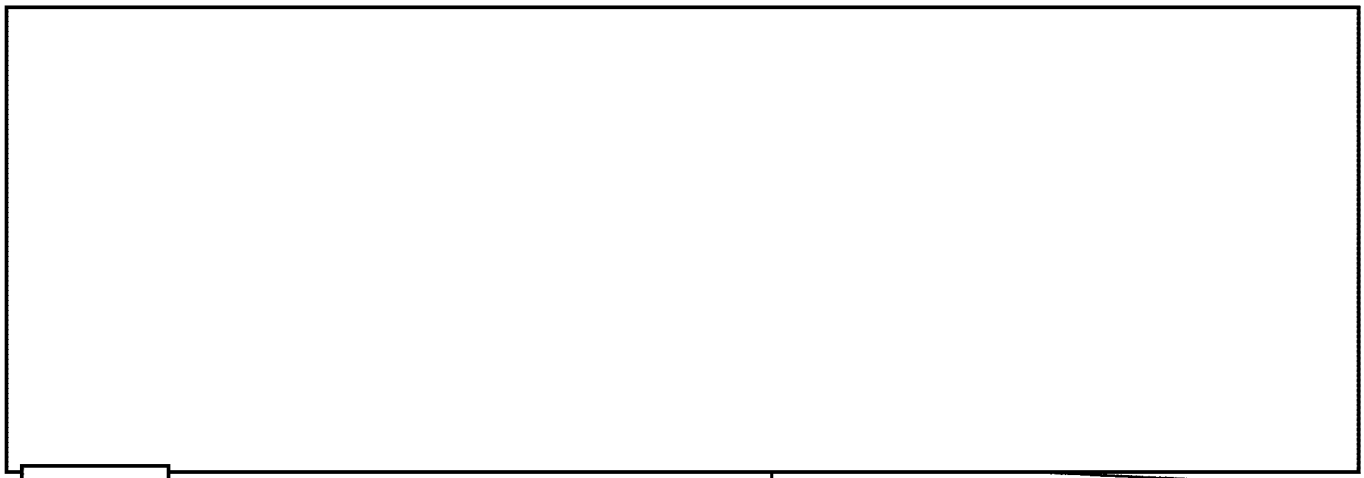
b5

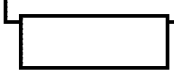


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

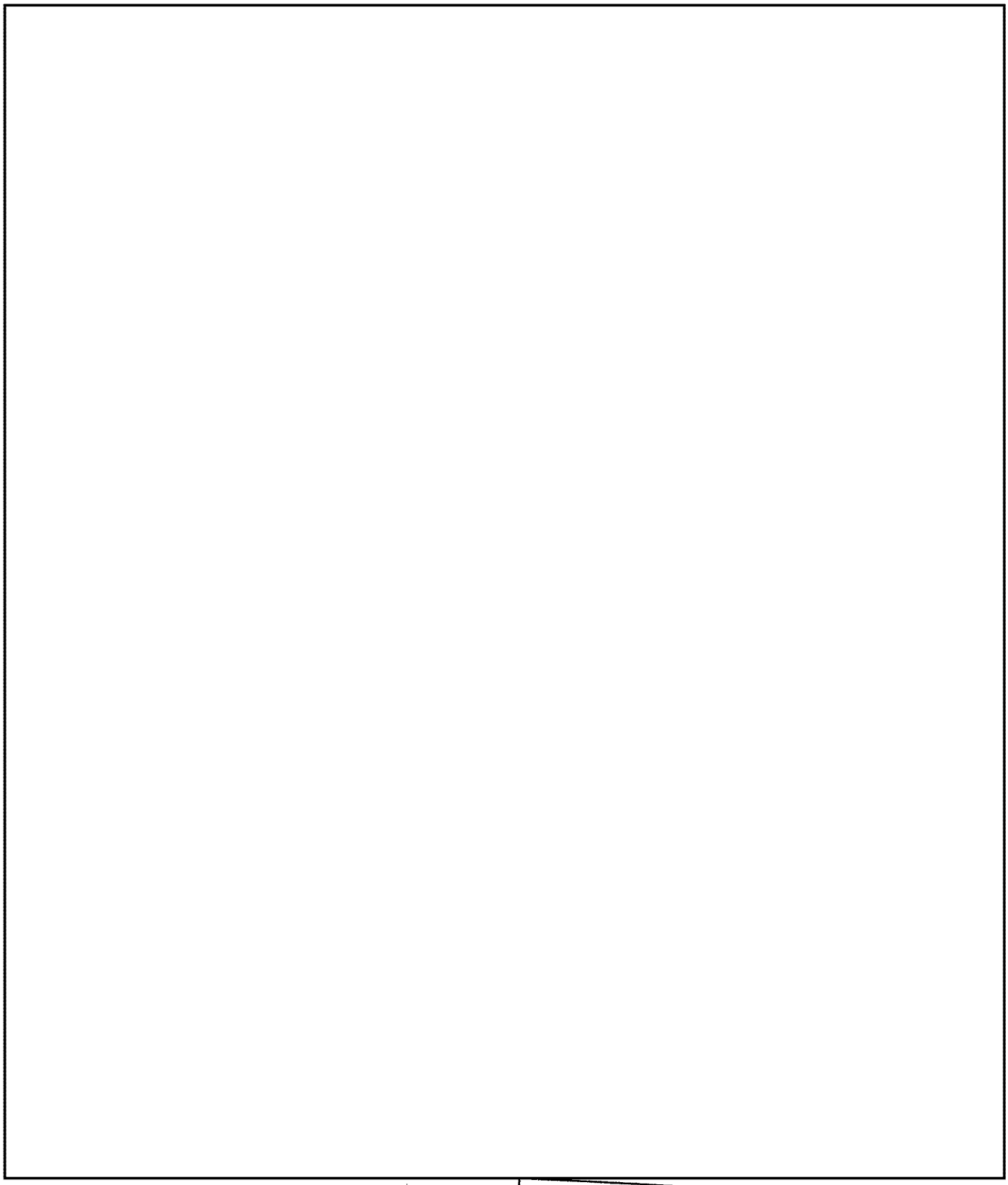






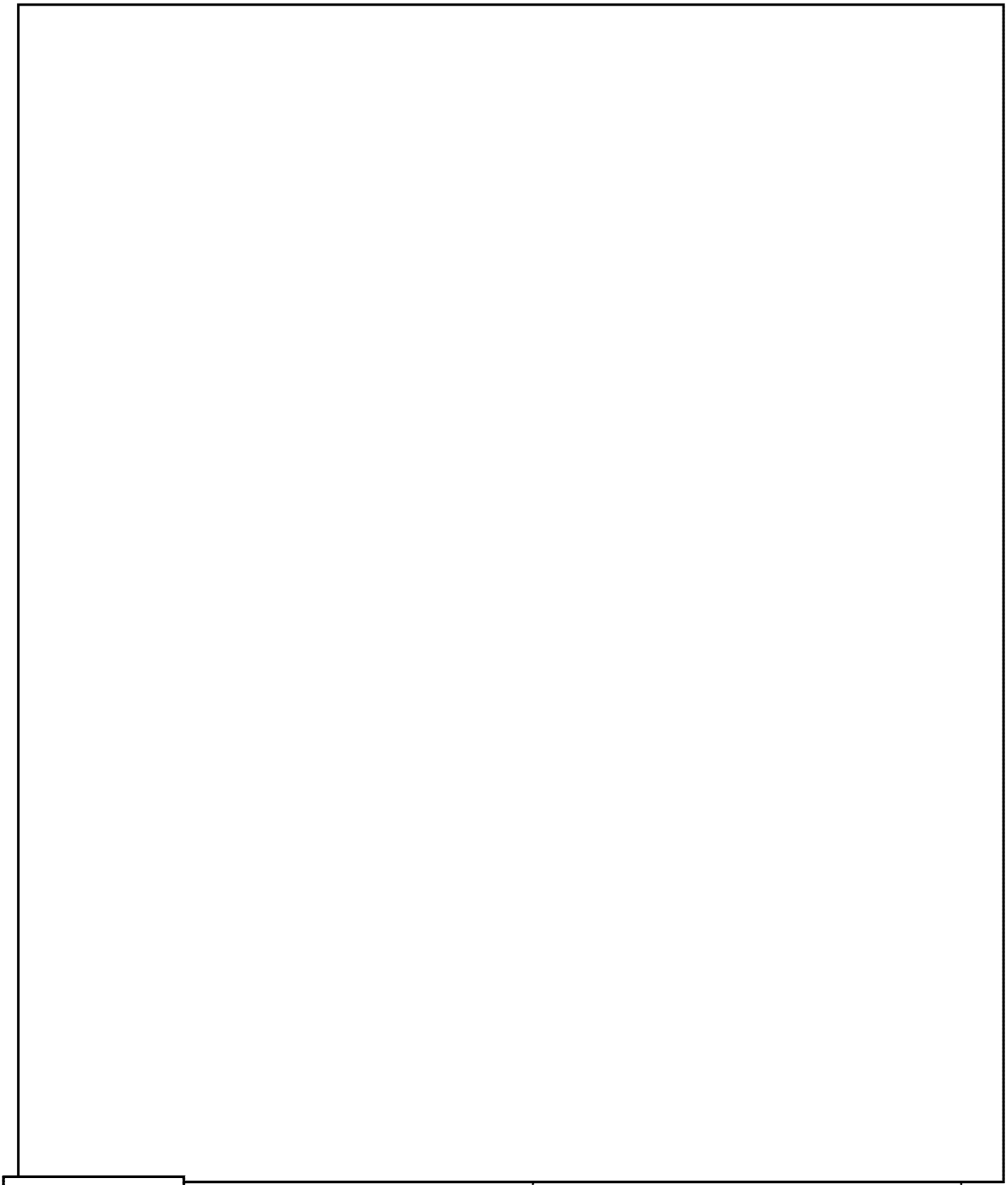
b5

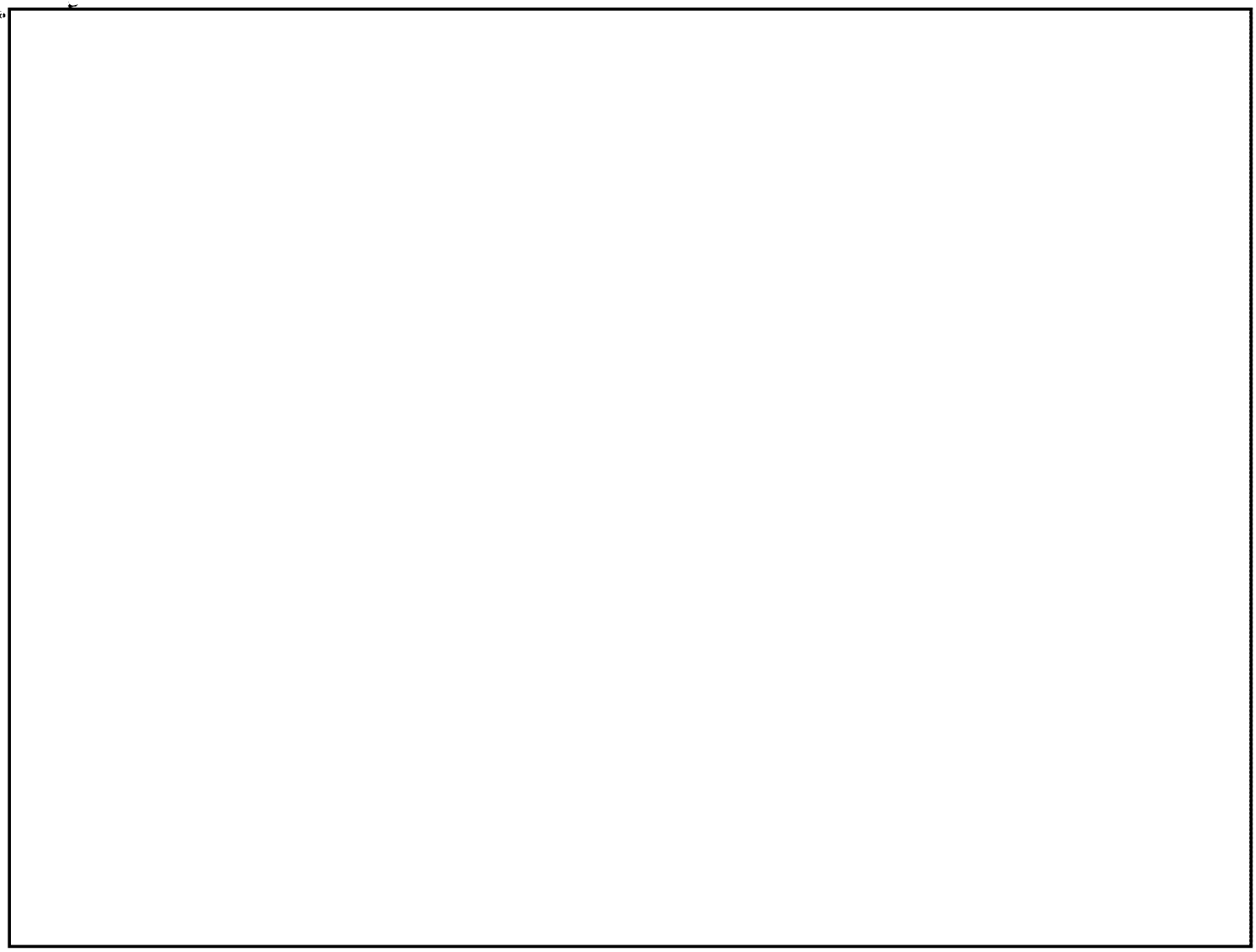
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT





PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

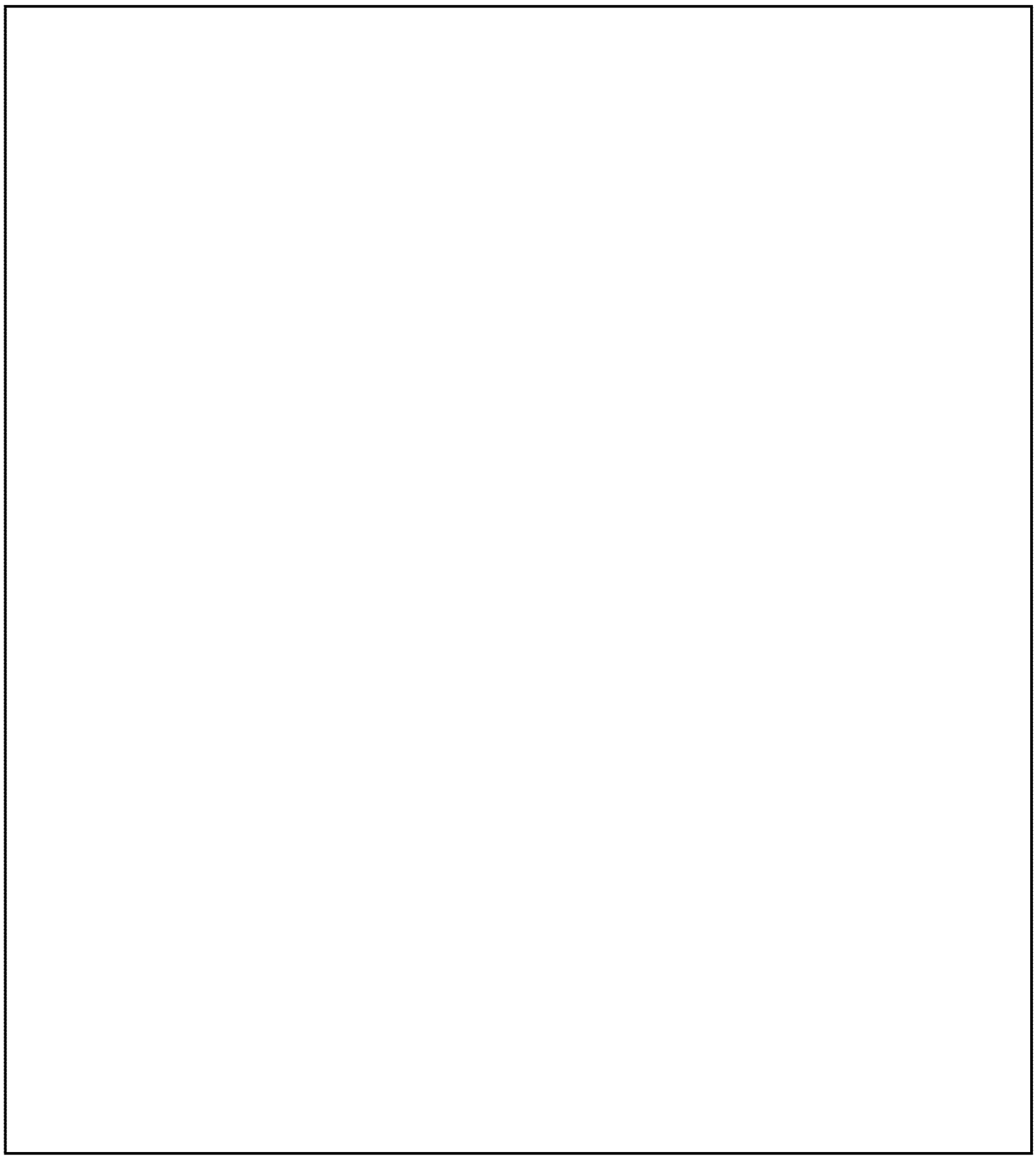
b5

7

Disclosure to the TTIC of Criminal Information obtained in International Terrorism (315) Cases

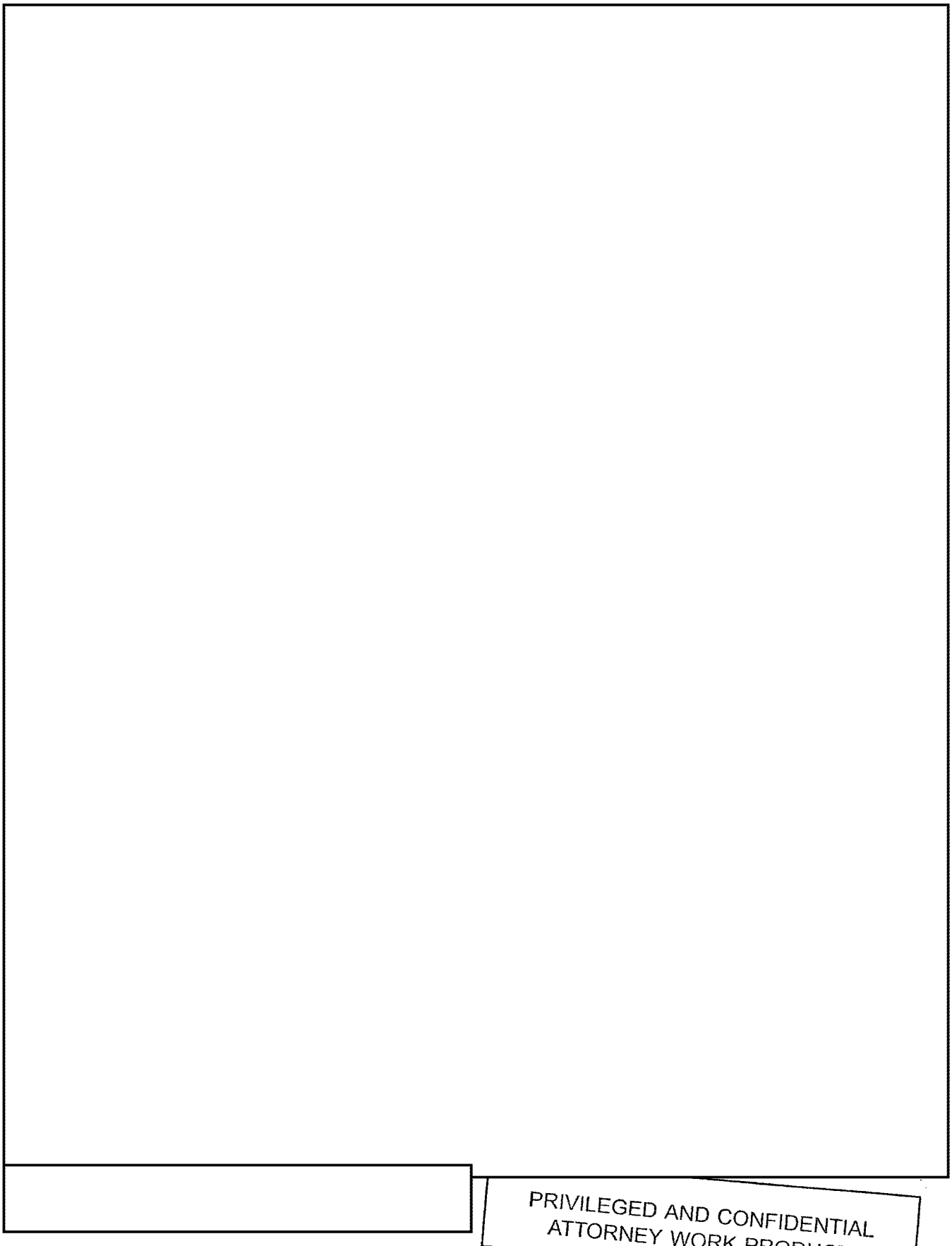
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

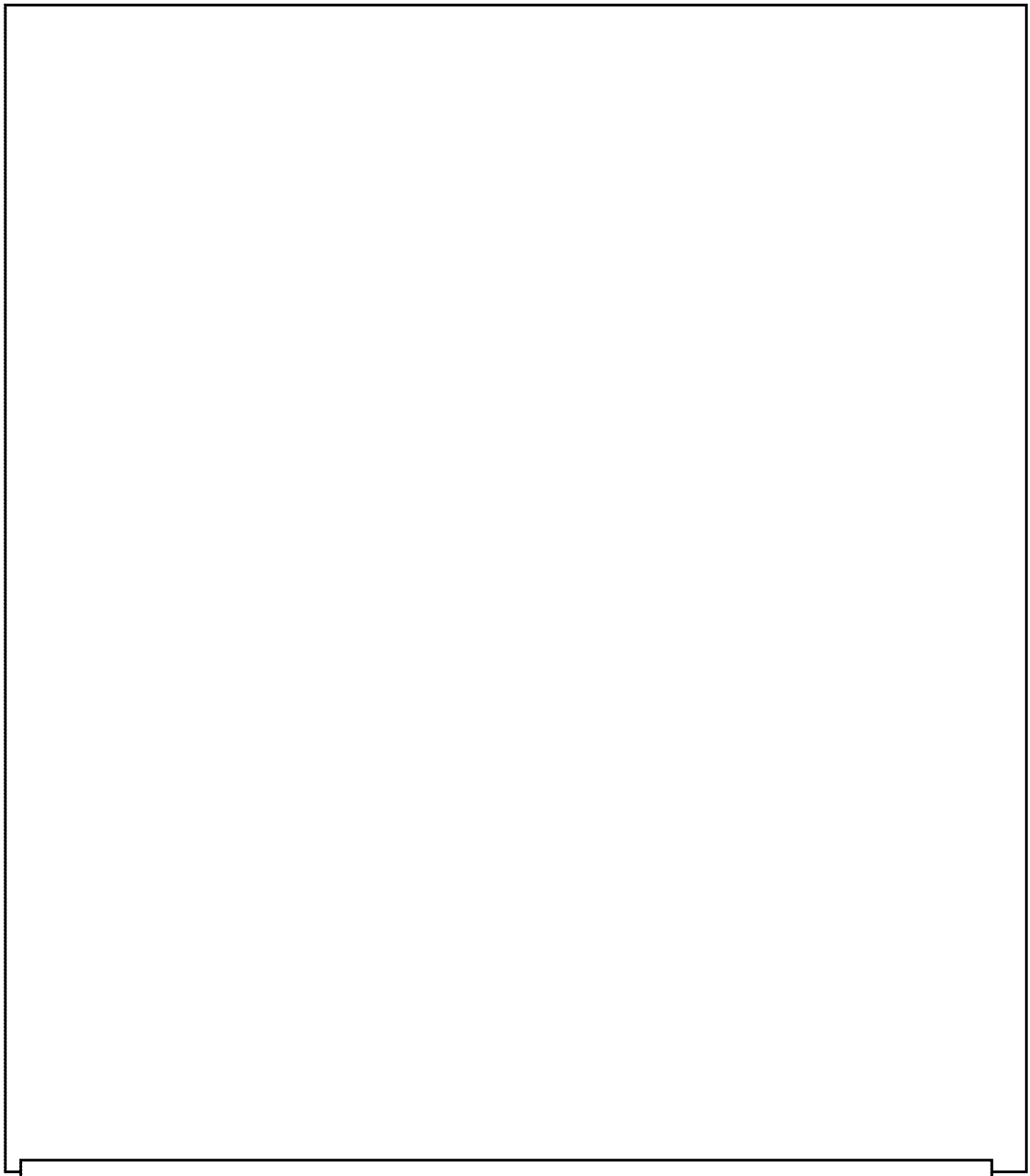
b5

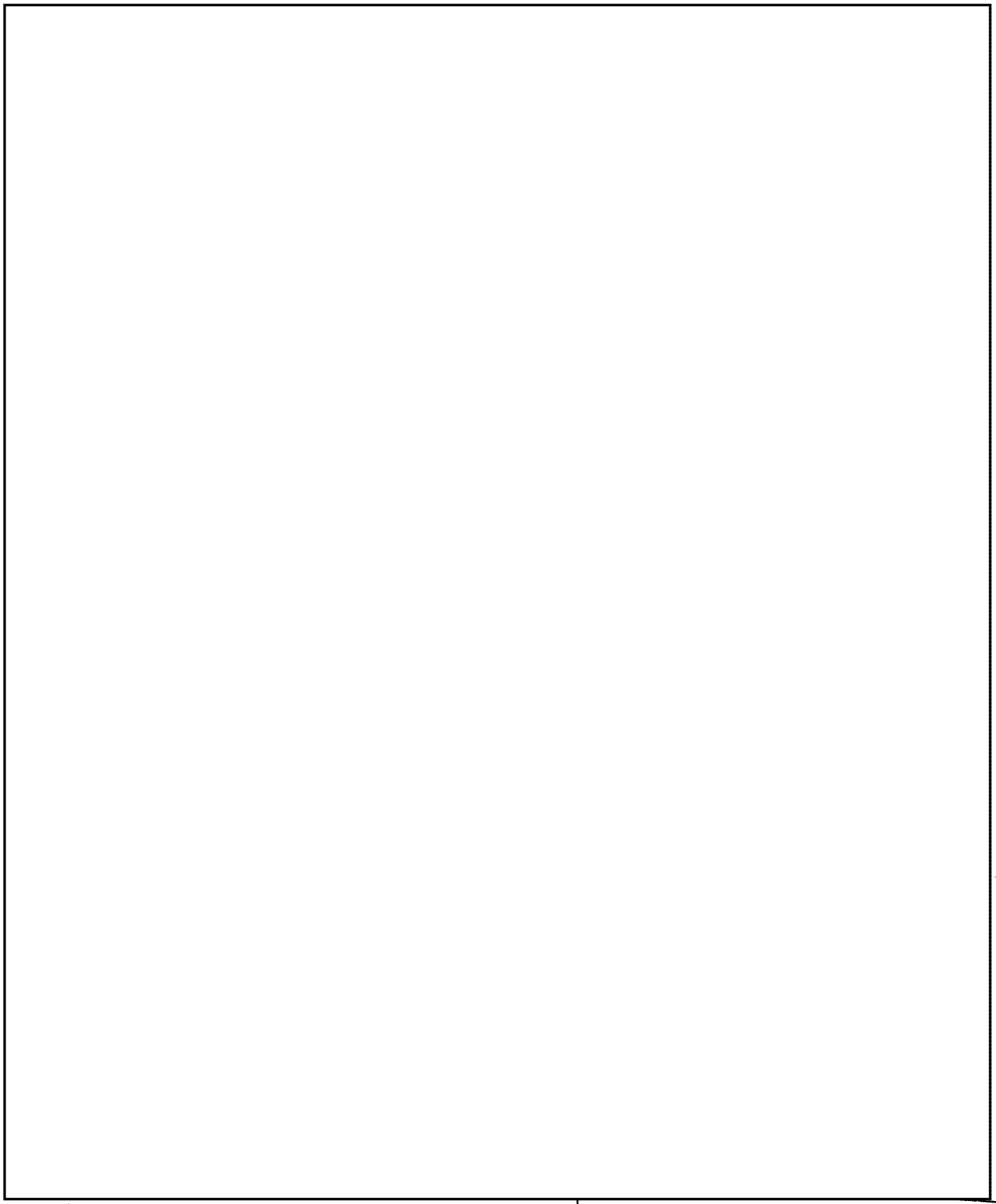


b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

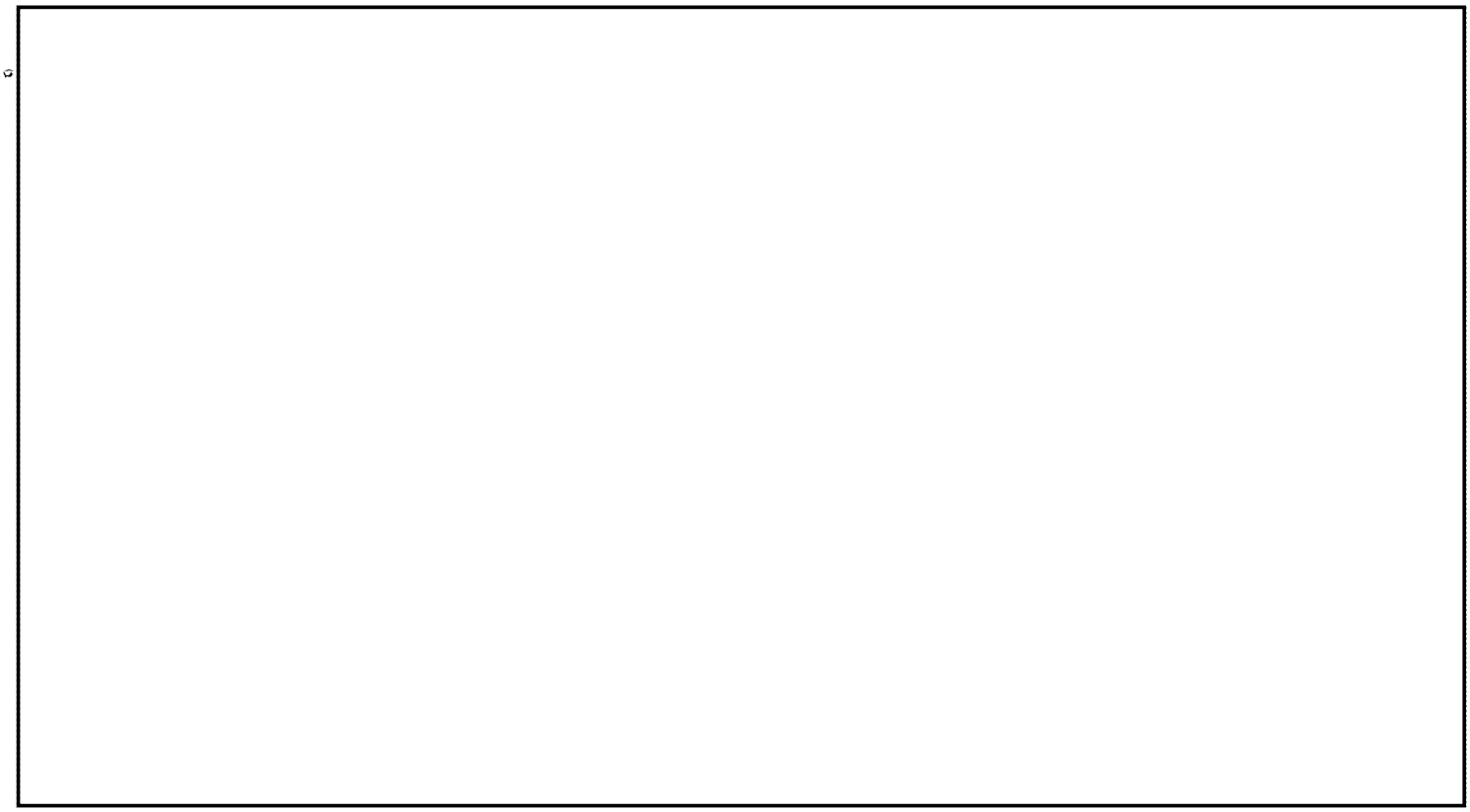






b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

7

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ-A1247863, 10/26/2001

DATE: 12-09-2005
CLASSIFIED BY 65179 DMH/LP 05-CV-0845
REASON: 1.4 ((C))
DECLASSIFY ON: 12-09-2030

From: Office of the General Counsel
NSLU/NSLB, Room 7975
Contact: National Security Law Unit, [redacted] b2

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E
[redacted] b6 b7C

Drafted By: [redacted] mjw

Case ID #: 66F-HQ-A1247863 (None)

Title: NEW LEGISLATION
REVISIONS TO FCI/IT LEGAL AUTHORITIES
FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

Synopsis: Summarizes recent changes to FISA statute and related legal authorities.

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" which significantly revises many legal authorities relating to counterterrorism. The Act, which consists of more than 150 sections, effects changes in national security authorities, the substantive criminal law, immigration law, money laundering statutes, victim assistance statutes, and other areas. [redacted] b5

[redacted]

~~SECRET~~

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

[redacted]

1. Sharing Grand Jury, Title III and Criminal Investigative Information

Section 203 first amends Federal Rule of Criminal Procedure 6(e) to permit the disclosure of grand jury information involving intelligence information "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section also requires subsequent notice to the Court of the agencies to which information was disseminated and adds a definition of "foreign intelligence information" to Rule 6(e). The Grand Jury portion of this Section (Section 203(a)) is not subject to the sunset provision.

Section 203 then amends Title III to allow the same sort of disclosure of Title III information when the matters involve foreign intelligence "to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section adds a definition of foreign intelligence information to Title III, and requires the Attorney General to develop procedures for the sharing of Grand Jury or Title III information that identifies a U.S. person.

Finally, Section 203 establishes that "notwithstanding any other law" it is lawful for criminal investigators to share foreign intelligence information obtained in the course of a criminal investigation with any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official, as above.

The intent of Section 203 is to eliminate barriers to the timely sharing of information between criminal investigators and other entities (the Intelligence Community, the INS, DoD, etc.) involved in the protection of the national security. The Section essentially gives the FBI full discretion to share criminal investigative information, regardless of its source, whenever it involves foreign intelligence information (which is defined to include all foreign intelligence, counterintelligence, and counterterrorism information).

Procedural Changes: FBI components in possession of information obtained through criminal investigative techniques that is also foreign intelligence information should arrange for the appropriate dissemination of the information. Dissemination to the Intelligence Community must be coordinated through the relevant NSD or CTD units at FBIHQ. When the DOJ issues procedures relating to the dissemination of U.S. person information, the field will receive additional guidance.

2. "Roving" FISA ELSUR Authority

Section 206 amends FISA to allow the Court to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in tradecraft designed to defeat ELSUR, such as by [redacted] the Court can issue an order directing "other persons, [redacted] etc., to effect the authorized electronic surveillance. Even if the target is not engaged in obvious tradecraft, we can obtain such an order as long as the target's actions may have the effect of thwarting surveillance. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. [redacted]

b1 (S)

b5

Procedural Changes: When the field wants to obtain roving ELSUR authority, the request for a FISA sent to FBIHQ should include specific facts that will allow the Court to find that the actions of the target may have the effect of thwarting the requested surveillance, absent the roving authority. Such facts could include examples of previous tradecraft by the target, by members of the target's group or service, or by others with training or background similar to that presumed for the target. DOJ/OIPR may issue more detailed guidance as experience with this provision grows.

3. Changes in the Duration of FISA Authority

Section 207 extends the standard duration for several categories of FISA orders. First, the section allow for ELSUR and search orders on non-U.S. person agents of a foreign power pled under Section 101(b)(1)(A) of FISA (i.e., officers and employees of foreign powers, including members of international terrorist groups) to run for an initial period of 120 days (instead of 90) and to be renewed for periods of one year. The section also extends the standard duration of physical search orders in all other cases (U.S. persons and non-officer/employee targets) from 45 to 90 days.

Procedural Changes: None are required. OIPR will transition existing coverages to the new durations as they come up for renewal.

4. Expansion of the FISA Court

In order to increase the availability of FISA judges, Section 207 expands the Court from seven judges to eleven judges, three of whom must reside in the Washington, D.C. area.

Procedural Changes: None are required.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

5. Changes in FISA Pen Register/Trap and Trace Authority

Section 214 makes a substantial revision to the standard for a FISA pen register/trap and trace. Prior to the Act, FISA pen registers required two showings: (1) relevance to an investigation, and (2) specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. Section 214 simply eliminates the second of the required showings. FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." b1 b5

This new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." Use of this technique is authorized [redacted] (S) Although the language differs somewhat from that used in the previous versions of the statute, [redacted] b5

The Section also inserts the language "provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Congress inserted this to indicate that the technique will not be used against U.S. persons who are merely exercising constitutionally protected rights. [redacted] b5

[redacted] b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

[redacted] For example, information concerning apparent associates or, or individuals in contact with, the subject of a investigation, may be relevant.

Procedural Changes: None are required. The field may continue to request FISA pen register/trap and trace authority through FBIHQ in the established manner. However, the requests now need only contain a brief statement explaining the nature of the investigation and the relevance to that investigation of the information sought through the pen register. NSLU and OIPR will develop additional guidance streamlining the process for requesting this authority.

6. Changes in FISA Business Records Authority

Section 215 changes the business records authority found in Title V of FISA. The old language allowed the FISA Court to issue an order compelling the production of certain defined categories of business records (the records of common carriers, public accommodations, vehicle rentals, and storage facilities) upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. Section 215 changes this standard to simple relevance (just as in the FISA pen register standard described above) and gives the Court the authority to compel production of "any tangible things (including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This is the same standard described above for Section 214.

In the past, the FBI has encountered situations in which the holders of relevant records refused to produce them absent a subpoena or other compelling authority. When those records did not fit within the defined categories for National Security Letters or the four categories then defined in the FISA business records section, the FBI had no means of compelling production. With the new language the FBI can seek a FISA court order for any such materials.

Procedural Changes: None are required. The field may continue to request business records orders through FBIHQ in the established manner. However, such requests may now seek production of any relevant information, and need only contain information establishing such relevance. NSLU and OIPR will develop additional guidance streamlining the process for requesting this authority.

7. Changes to "Primary Purpose" Standard in FISA

Sections 218 and 504 clarify the "primary purpose" issue in the FISA statute. In its prior form, the FISA required a certification that foreign intelligence be "the" purpose of the requested authority. The FISA Court interpreted this to mean that foreign intelligence, as opposed to criminal prosecution, had to be the "primary"

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

purpose of the requested authority. Thus, interaction between FBI personnel involved in a FISA and criminal prosecutors could call into question the primary intelligence purpose of the FISA (by indicating a purpose different from foreign intelligence). As a result, FISA pleadings have often contained detailed accounts of all communication with criminal prosecutors in cases involving FISA.

Section 218 changes FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amends FISA to allow that personnel involved in a FISA may consult with law enforcement officials to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose."

These changes are meant to allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk. As such, these changes address extraordinarily complex issues that have long occupied the FISA Court and DOJ. FBIHQ expects that DOJ shortly will issue revised policy on these topics.

Procedural Changes: None are required at present. The field should be aware that greater consultation with prosecutors is now possible, but, given the continuing uncertainty surrounding these issues, should continue to coordinate such consultation through FBIHQ. Additional guidance will be issued.

8. Civil Liability for Unauthorized Disclosure

Section 223 establishes civil liability for certain unauthorized disclosures, including unauthorized disclosures of FISA information. In reference to FISA, this is simply an expansion of existing civil liability, and should not significantly affect operations (since unauthorized disclosure of FISA information is already subject to more severe criminal penalties).

Procedural Changes: None are required. OGC may issue a more detailed analysis of this provision at a later date.

9. Immunity for Compliance with FISA

Section 225 grants providers of wire or electronic communication service, landlords, custodians, and other persons with immunity from civil liability for complying with the requirements of FISA. This provision simply clarifies that persons assisting the FBI in the execution of a FISA order are not at risk of civil lawsuits.

Procedural Changes: None are required.

10. Disclosure of Foreign Intelligence Information to the DCI

Section 905 establishes an affirmative requirement, subject to certain exceptions, that federal law enforcement components must expeditiously disclose to the Director of Central Intelligence any foreign intelligence acquired in the course of criminal investigations. The Attorney General will, within the next six months, develop guidelines to govern such disclosures.

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ-A1247863, 10/26/2001

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in FCI/IT operations and to other division personnel as appropriate.

♦♦

b6
b7C

From: [redacted]
Sent: Monday, February 09, 2004 10:55 AM
To: [redacted]
Cc:
Subject: RE: TTIC

Federal Tax Records

The FBI is authorized to receive federal tax returns and return information, pursuant to 26 USC §6103(i), upon grant of ex parte order by Federal District Court Judge, or upon written request signed by the Director, FBI (for limited information- not returns). [redacted]

[redacted] b5

[redacted] b5

Title III Derived Information

18 USC 2517(6) allows "foreign intelligence" "counterintelligence" or "foreign intelligence information" obtained via a Title III intercept to be disclosed to any Federal law enforcement or intelligence official (among others) to assist in the performance of his duties. [redacted] b5

[redacted] The Attorney General Guidelines for disclosure of this information (implementation of Patriot Act Sections 203 and 905(a)) require that the prosecuting official be consulted prior to disclosure (except for threat information), and that information identifying US Persons be so marked. Use restrictions may be added if deemed necessary.

Medical Records

The Medical Records Privacy Regulations issued pursuant to HIPAA do not regulate the FBI's handling or disclosure of medical records, they only apply to health care providers, health plans (insurance companies) and health care clearinghouses (billing companies).

Protected health information (a patient's medical records) ~~obtained by the FBI during a health care~~ fraud investigation may not be used for unrelated civil, administrative, or criminal investigations of a

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

non-health oversight matter, except when the balance of relevant factors weighs clearly in favor of its use (as determined by the DAG, DOJ), pursuant to Executive Order 13181 (Dec. 20, 2000). In addition, medical records obtained with an administrative subpoena pursuant to 18 USC 3486 (health care fraud cases) may not be used against the individual in an unrelated administrative, civil or criminal action or investigation, without a court order. [redacted] b5

[redacted]

Drug and alcohol abuse records can only be obtained by the FBI with the patient's consent, or with a court order. If the FBI obtained the records with the patient's consent, the FBI must also have the patient's consent to authorize any redisclosure. 42 CFR 2.32. If a court order was used, further disclosure by the FBI is governed by the terms of that court order. 42 USC §290dd-2(b)(2)(C). Without such explicit authorization, no drug/alcohol abuse records may be disclosed to TTIC.

[redacted] b5

-----Original Message-----
From: [redacted] b6
Sent: Monday, February 02, 2004 4:12 PM b7C
To: [redacted] b5
Cc: b6
Subject: TTIC b7C

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

11 April 2002. Thanks to Declan McCullagh.
Source: http://www.politechbot.com/docs/ashcroft.info.sharing.041102.pdf (215KB)

See DoJ press release:

http://www.usdoj.gov/opa/pr/2002/April/02_ag_211.htm

[5 pages.]

Office of the Attorney General

Washington, D.C. 20530

April 11, 2002

MEMORANDUM FOR THE DEPUTY ATTORNEY GENERAL, THE ASSISTANT ATTORNEY GENERAL FOR THE CRIMINAL DIVISION, THE ASSISTANT ATTORNEY GENERAL FOR LEGAL POLICY, THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION, THE COMMISSIONER OF THE IMMIGRATION AND NATURALIZATION SERVICE, THE ADMINISTRATOR OF THE DRUG ENFORCEMENT ADMINISTRATION, THE DIRECTOR OF THE EXECUTIVE OFFICE OF UNITED STATES ATTORNEYS, THE DIRECTOR OF THE MARSHALS SERVICE, AND THE DIRECTOR OF THE FOREIGN TERRORIST TRACKING TASK FORCE.

FROM: THE ATTORNEY GENERAL *[Signed]*

SUBJECT: Coordination of Information Relating to Terrorism

The prevention of terrorist activity is the overriding priority of the Department of Justice. By memoranda dated November 8 and 13, 2001, I directed Department components to review their policies and procedures to ensure information sharing, information analysis, and coordination of activities with federal, state and local agencies to prevent acts threatening public safety and national security. The Deputy Attorney General has reported to me the specific actions taken to implement those directives. I commend you on the substantial progress the Department has achieved in analyzing information, sharing intelligence and coordinating activities in the multi-front effort to combat terrorism.

I am hereby directing you to undertake further action to institutionalize the Department's ongoing efforts to coordinate information and activities to prevent and disrupt terrorist activities.

1. Expand Terrorist Information in Law Enforcement Databases.

The Federal Government maintains a number of databases that provide real-time information to officials in foreign diplomatic outposts, at border points of entry, and for interior domestic law enforcement. Expansion of information in such databases relating to known and suspected terrorists will greatly enhance the ability of federal, state, and local officials to prevent terrorists from obtaining visas to enter the United States, to deny them entry into our borders, to detect and apprehend those already in the country, and to gather intelligence on the plans and activities of terrorist conspiracies. Accordingly, I hereby direct all investigative components within the Department of Justice to establish procedures to

provide, on a regular basis and in electronic format, the names, photographs (if available), and other identifying data of all known or suspected terrorists for inclusion in the following databases:

- The Department of State TIPOFF System. This system is designed to detect known or suspected terrorists who are not U.S. citizens as they apply for visas overseas or as they attempt to pass through U.S., Canadian, and Australian border entry points. Expanding terrorist information in the database will preclude the issuance of visas to known terrorists; warn U. S. diplomatic posts of the security risk posed by certain applicants; and alert intelligence and law enforcement agencies of the travel plans of suspected terrorists.

- The FBI National Crime Information Center (NCIC). The NCIC is the nation's principal law enforcement automated information sharing tool. It provides on-the-street access to information to over 650,000 U.S. local, state, and federal law enforcement officers. The inclusion of terrorist information in this powerful database will assist in locating known foreign terrorists who have entered the U.S. undetected, warn law enforcement officers of a potential security risk, and alert intelligence and law enforcement agencies of the presence of a suspected terrorist at a specific location and time. Agencies contributing terrorist information should establish procedures and protocols for direct electronic input of the data into NCIC, observing applicable restrictions on the entry of classified information into the system. To expand further local and state law enforcement access to relevant terrorist information, the FBI shall establish procedures with the Department of that that will enable, on a recurring basis, the inclusion of qualifying TIPOFF data into NCIC. The FBI shall establish procedures that inform law enforcement officers what action should be taken when encountering suspected terrorists. Furthermore, the NCIC must properly characterize individuals as either suspected terrorists or known terrorists, with the latter designation reserved for individuals against whom sufficient evidence exists to justify such a determination.

- The U.S. Customs Service Interagency Border Inspection System (IBIS). This system is the primary automated screening tool used by both the Immigration and Naturalization Service (INS) and U.S. Customs Service at ports-of-entry. The inclusion of terrorist data in this integrated database will help preclude the entry of known and, suspected terrorists into the U.S., warn inspectors of a potential security threat, and alert intelligence and law enforcement agencies that a suspected terrorist is attempting to enter the U.S. at a specific location and time. Such information on known or suspected foreign terrorists must be placed in IBIS unless it is already accessible through an automated IBIS query of NCIC.

The procedures established for providing information to the databases listed above may allow for case-by-case exceptions where the component head or his responsible designee determines that disclosure would compromise classified information, jeopardize an investigation, or compromise a confidential source.

2. Coordinate Foreign Terrorist Information.

The international response to the September 11th attacks has been defined by multilateral cooperation and resolve to restore security and liberty to freedom-loving people of the world. The success of the response has depended in large part on improved sharing among governments of information relating to terrorists, their associates, and their activities. Continued vigilance against international terrorist conspiracies requires procedures to institutionalize such information coordination. Accordingly, I hereby direct the FBI, through its Legal Attaches, to establish procedures to obtain on a regular basis the fingerprints, other identifying information, and available biographical data of all known or suspected foreign terrorists who have been identified and processed by foreign law enforcement agencies. The FBI shall also coordinate with the Department of Defense to obtain, to the extent permitted by law, on a

regular basis the fingerprints, other identifying information, and available biographical data of known or suspected foreign terrorists who have been processed by the U.S. Military. Such information shall be placed into the Integrated Automated Fingerprint Identification System (IAFIS) and other appropriate law enforcement databases to assist in detecting and locating foreign terrorists.

3. Establish Secure System for Information Coordination with State and Local Partners.

The various information systems described above are databases, triggered by a name query, that serve as an alert mechanism and pointer index. Effective information coordination requires more sophisticated mechanisms for expanded searches, multipoint information flow, and integrated analysis. Federal agencies have the benefit of classified systems that enable keyword searches of relevant documents, secure e-mail, and other important collaborative information sharing tools, However, there is no corresponding national system with comparable capability for integrated information coordination on counterterrorism with and among state and local law enforcement agencies.

By memorandum of November 13, 2001, I directed all U.S. Attorneys to develop protocols for coordinating information to, from, and among our state and local par in law enforcement. I encouraged the use, where practicable, of technologies already available and currently in use by the Department to facilitate information-sharing. I hereby direct the Deputy Attorney General to coordinate among the applicable components the development of a secure but unclassified web-based system to enable local, state, and federal users to post, retrieve, and read information, restrict access to certain products, send secure e-mail, and receive automatic e-mail notifications when new items are posted. This integrated system should allow for future capabilities, such as imagery and photographs, instant messaging and database access and restricted access to classified information at least at the Secret level and ideally in higher classifications.

4. Analyze Foreign Terrorist Data.

On October 30, 2001, the President directed that the Department establish the Foreign Terrorist Tracking Task Force (FTTTF). The mission of the FTTTF is to keep foreign terrorists and their supporters out of the United States by providing critical and timely information to border control and interior enforcement agencies and officials. To do so requires electronic access to large sets of data, including the most sensitive material from law enforcement and intelligence sources. Analyzing such data will enable the FTTTF to discern patterns and probabilities of terrorist activities.

I hereby direct the FTTTF to identify the agency information systems and data sets needed to fulfill its mission. Each agency is to provide to the FTTTF unfiltered, timely and electronic access to the information systems and data sets deemed relevant by the Director of the FTTTF, subject to any legal restrictions on the sharing of such information.

5. Standardize Procedures for Sharing of Sensitive Information.

Section 203 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, authorizes the sharing of foreign intelligence and counterintelligence information obtained as part of a criminal investigation, including through grand jury proceedings and Title III electronic surveillance, with relevant Federal officials to assist in the performance of their duties. The officials receiving such information may use it only as necessary in the conduct of their official duties and subject to any limitations on the unauthorized disclosure of such information. The Criminal Division has developed and distributed model forms to be used to notify the supervising court when grand jury information has been shared

pursuant to section 203.

Section 905 of the USA PATRIOT Act requires the Department and other Federal agencies with law enforcement responsibilities to share expeditiously foreign intelligence obtained in the course of a criminal investigation with the Director of Central Intelligence, subject to limitations otherwise provided by law and exceptions delineated in regulations to be issued by the Department. In the types of criminal cases in which foreign intelligence information is commonly encountered -- including terrorism, drug trafficking, and organized crime investigations -- strong relationships for information-sharing and coordination w the Intelligence Community are already in place.

I hereby direct the Assistant Attorney General for Legal Policy, in consultation with the Criminal Division, FBI, and other relevant components, to draft, for my consideration and promulgation, procedures, guidelines, and regulations to implement sections 203 and 905 of the USA PATRIOT Act in a manner that makes consistent and effective the standards for sharing of information, including sensitive or legally restricted information, with other Federal agencies. Those standards should be directed toward, consistent with law, the dissemination of all relevant information to Federal officials who need such information in order to prevent and disrupt terrorist activity and other activities affecting our national security. At the same time, the procedures, guidelines, and regulations should seek to ensure that shared information is not misused for unauthorized purposes, disclosed to unauthorized personnel, or otherwise handled in a manner that jeopardizes the rights of U.S. persons, and that its use does not unnecessarily affect criminal investigations and prosecutions. The standards adopted will govern the coordination of information directed by this memorandum, and well as other voluntary or mandated sharing of criminal investigative information.

* * *

The September 11 attacks demonstrate that the war on terrorism must be fought and won at home as well as abroad. To meet this continuing threat, law enforcement officials at all levels of government -- federal, state, and local -- must work together, coordinating information and leveraging resources in the joint effort to prevent and disrupt terrorist activity. You have worked hard and accomplished much in this common fight, but more remains to be done to help secure America and protect her people. I thank you for your continued service, dedication, and cooperative spirit in this time of continuing national need.

Transcription and HTML by Cryptome.

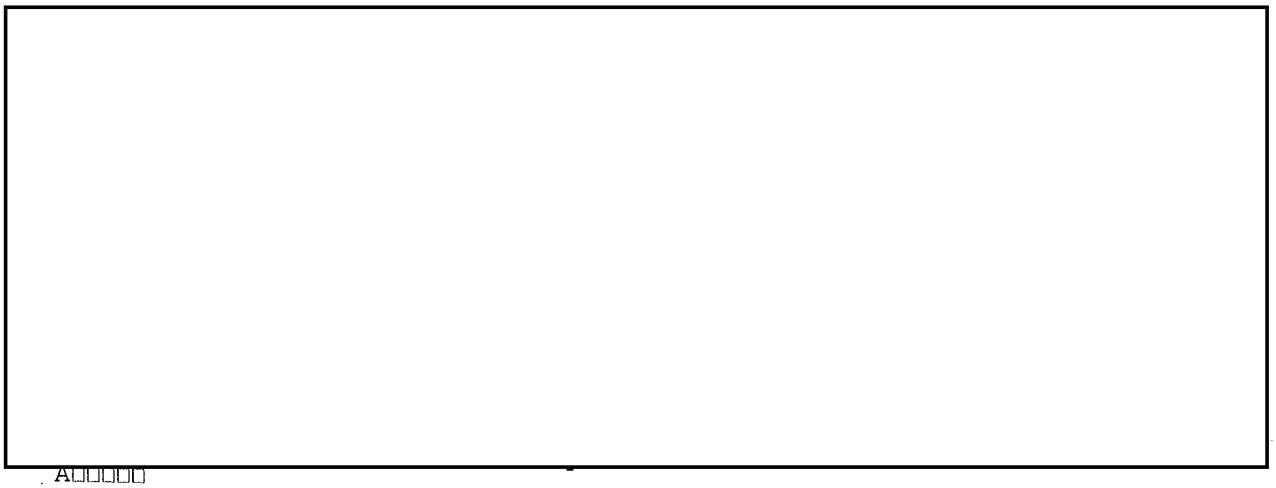
ÄÁ□Ø Ø □□ÁTerrorist DNA database

Ð□Ð□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□°□□□`
b5 □□h□À□□□p□È□ x Ð (#€%Ø'0*^,à.81▯3è5@8~:õ<H? AøCPF¨H□KXM°O□R`T V□Yh[À]
□`□□□□□□□□□□□□□□□□□□□□□□□°□Ð□□ [redacted]

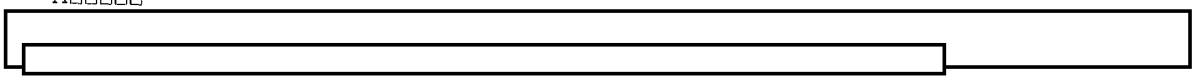
[redacted] b5 b6 b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

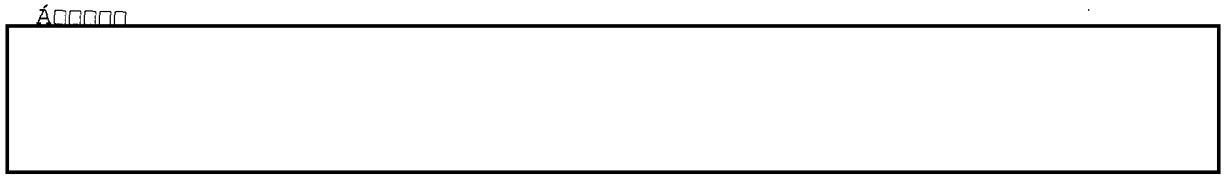


A□□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□Á
Á□□□□□



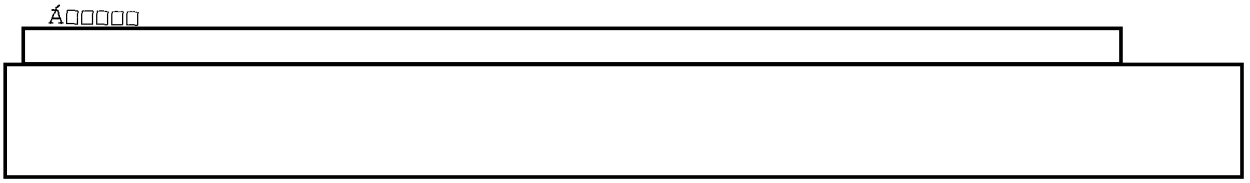
b5

Á□□□□□



b5

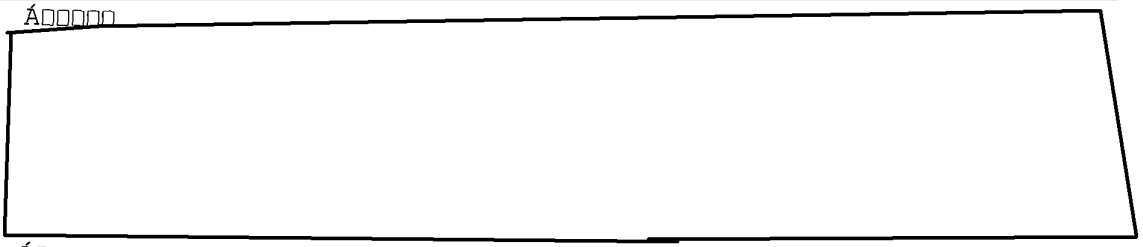
Á□□□□□



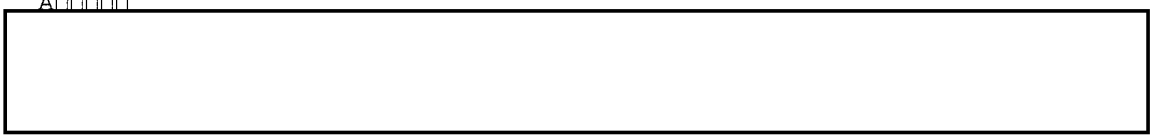
b5

b5

Á□□□□□



Á□□□□□



b5

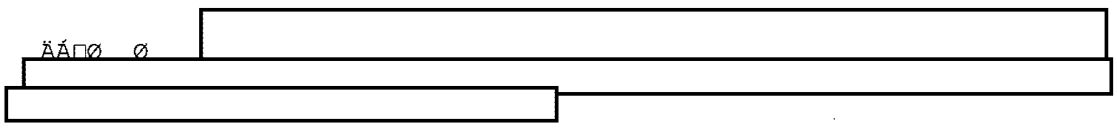
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

[redacted]

b5
b6
b7C

Ð□Ð□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□Ø ÿÿÿ
ÿÿ
Ã ÿÿ□□□□□□□□□□□□□□□□□□□□□□□□□□□°·□Ð□□Ð

ÃCC:Ä



b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-05-2005 BY 65179 DMH/JHF 05-CV-0845

RE sharing DNA profiles with [redacted].txt

From: [redacted] (Div09) (FBI) b6
Sent: Tuesday, May 04, 2004 6:35 PM b7C
To: [redacted] (LD) (FBI) b7D
Cc:
Subject: RE: sharing DNA profiles with [redacted]

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

b2
b5
b6
b7C
b7E

[redacted]

RE sharing DNA profiles with [redacted] txt

b2
b5
b6
b7C
b7E
b7D

[redacted]

Hope this helps--need to run to my bus.....

-----Original Message-----
From: [redacted] (LD) (FBI)
Sent: Tuesday, May 04, 2004 1:25 PM
To: [redacted] (Div09) (FBI)
Subject: FW: sharing DNA profiles with [redacted]

b6
b7C
b7D

UNCLASSIFIED
NON-RECORD

Hi [redacted] -

[redacted]

b2
b6
b7C
b7E

Thanks -
[redacted]

-----Original Message-----
From: [redacted]
Sent: Wednesday, April 07, 2004 1:47 PM
To: [redacted] (Div09) (FBI)
Subject: sharing DNA profiles with [redacted]

b6
b7C
b7D

Expires After: 7/6/2004 00:00

RE sharing DNA profiles with [redacted].txt

Hi [redacted]:

Recently I was contacted by [redacted] of CJIS concerning [redacted]

b2
b5
b6
b7C
b7D
b7E

Thanks, [redacted]

UNCLASSIFIED

UNCLASSIFIED

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

From: [redacted] (Div09) (FBI)
Sent: Monday, April 19, 2004 9:17 AM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: RE: Restrictions on sharing information with TTIC

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

[redacted]

b5

-----Original Message-----
From: [redacted] (FBI)
Sent: Thursday, March 04, 2004 3:19 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: Restrictions on sharing information with TTIC

b6
b7C

UNCLASSIFIED
NON-RECORD

Section 203(d) of the Patriot Act provides that "Notwithstanding any other provision of law" it is lawful to share foreign intelligence or counterintelligence (as defined in 50 USC 401a) or foreign intelligence information obtained as part of a criminal investigation with any federal law enforcement, intelligence, protective immigration, national defense, or national security official in order to assist the receiving official in his official duties. The receiving official may use the information only as necessary in the conduct of his official duties subject to any limitation on the unauthorized disclosure of such information.

b5

[redacted]

UNCLASSIFIED

UNCLASSIFIED

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

SECRET

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 10-06-2005
CLASSIFIED BY 65179 DMH/SHE 05-CV-0845
REASON: 1.4 (C , D)
DECLASSIFY ON: 10-06-2030

OGA info REQUIRES CONSULTATION w/OGA per ONSITE LIAISON

From: [redacted] b6
Sent: Tuesday, October 21, 2003 12:47 PM b7C
To: [redacted] b5
Cc: [redacted] b6
[redacted] b7C
Subject: SSCRET Material attached RE: Foreign Sharing Authority
SECRET Material attached

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, October 21, 2003 12:04 PM
To: [redacted]
Subject: FW: Foreign Sharing Authority

DATE: 12-05-2005
CLASSIFIED BY 65179/DMH/LP/DK 05-CV-0845
REASON: 1.4 (C,D)
DECLASSIFY ON: 12-05-2030

b5
b6
b7C

[redacted]

-----Original Message-----
From: [redacted] b6
Sent: Tuesday, October 21, 2003 11:58 AM b7C
To: [redacted] BOWMAN, MARION E.; [redacted]
Cc: [redacted] Briese, M Chris;
[redacted]
Subject: RE: Foreign Sharing Authority

[redacted] b5
b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

SECRET

b6
b7C

Thanks,

[redacted]

-----Original Message-----
From: [redacted] b6
Sent: Tuesday, October 21, 2003 9:54 AM b7C
To: BOWMAN, MARION E.;
Cc: Briese, M Chris;
Subject: RE: Foreign Sharing Authority

[redacted] b5 b6 b7C

-----Original Message-----
From: [redacted]
Sent: Tuesday, October 21, 2003 8:57 AM
To: BOWMAN, MARION E.;
Cc: Briese, M Chris; b6 b7C
Subject: RE: Foreign Sharing Authority

Spike--

[redacted] b5

[redacted] b1 b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b1
b5

[redacted] (S)

-----Original Message-----
From: BOWMAN, MARION E.
Sent: Tuesday, October 21, 2003 5:14 AM
To:
Cc: Briese, M Chris;
Subject: RE: Foreign Sharing Authority

b5
b6
b7C

[redacted]

-----Original Message-----
From:
Sent: Monday, October 20, 2003 5:41 PM
To:
Cc: BOWMAN, MARION E.; Briese, M Chris;
Subject: Foreign Sharing Authority

b6
b7C

[redacted]

b5
b6
b7C
b7D

Thanks,

[redacted]

DRAFT 10/20/2003

b5

FBI Authority to Share Information with Foreign Governments

[redacted] (S)

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

(U)

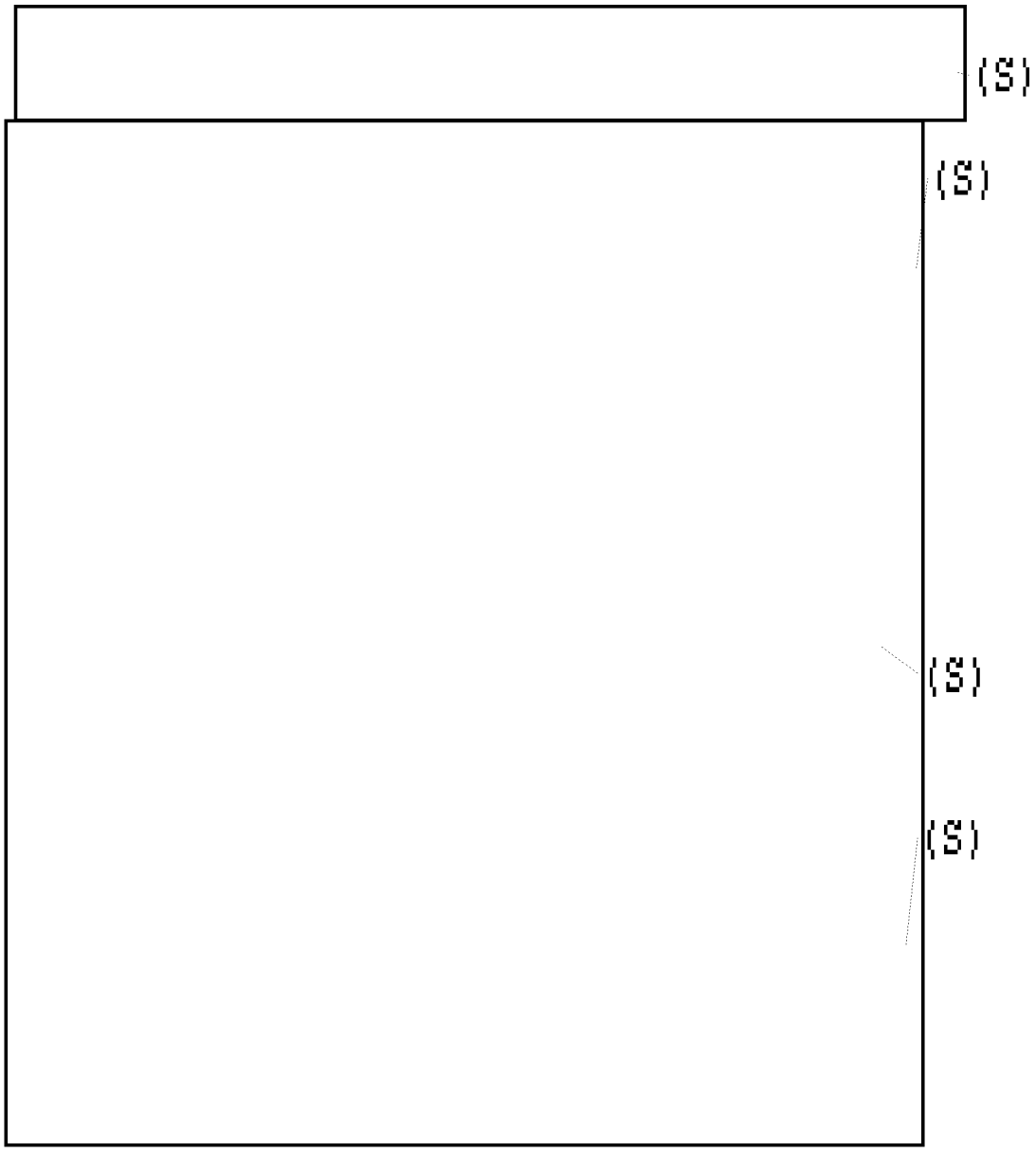
b1
b5

(S)

b1
b5
b2
b7D

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b1
b2
b7D
b5

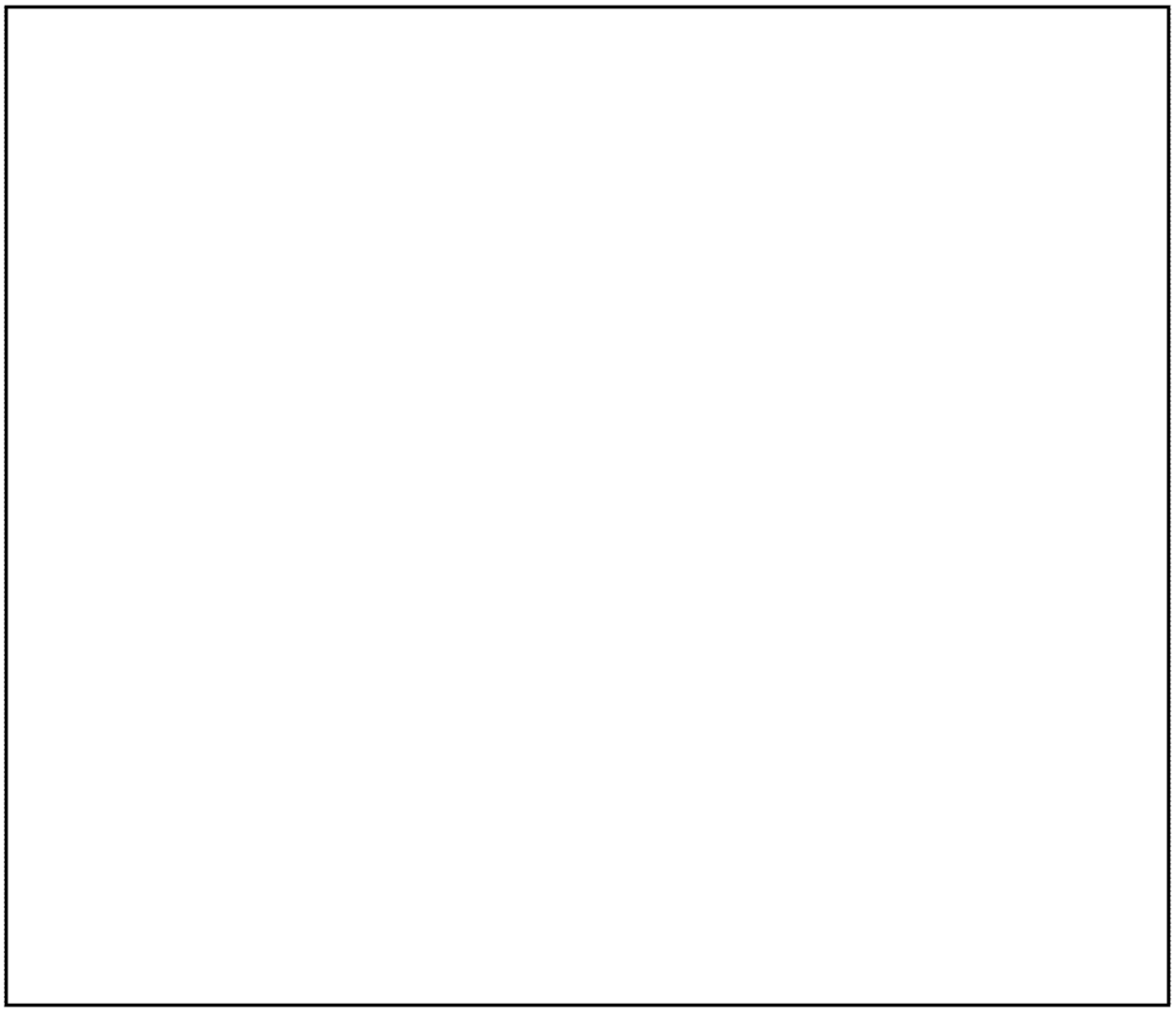


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

DRAFT10/14/04

b5

b5



b5

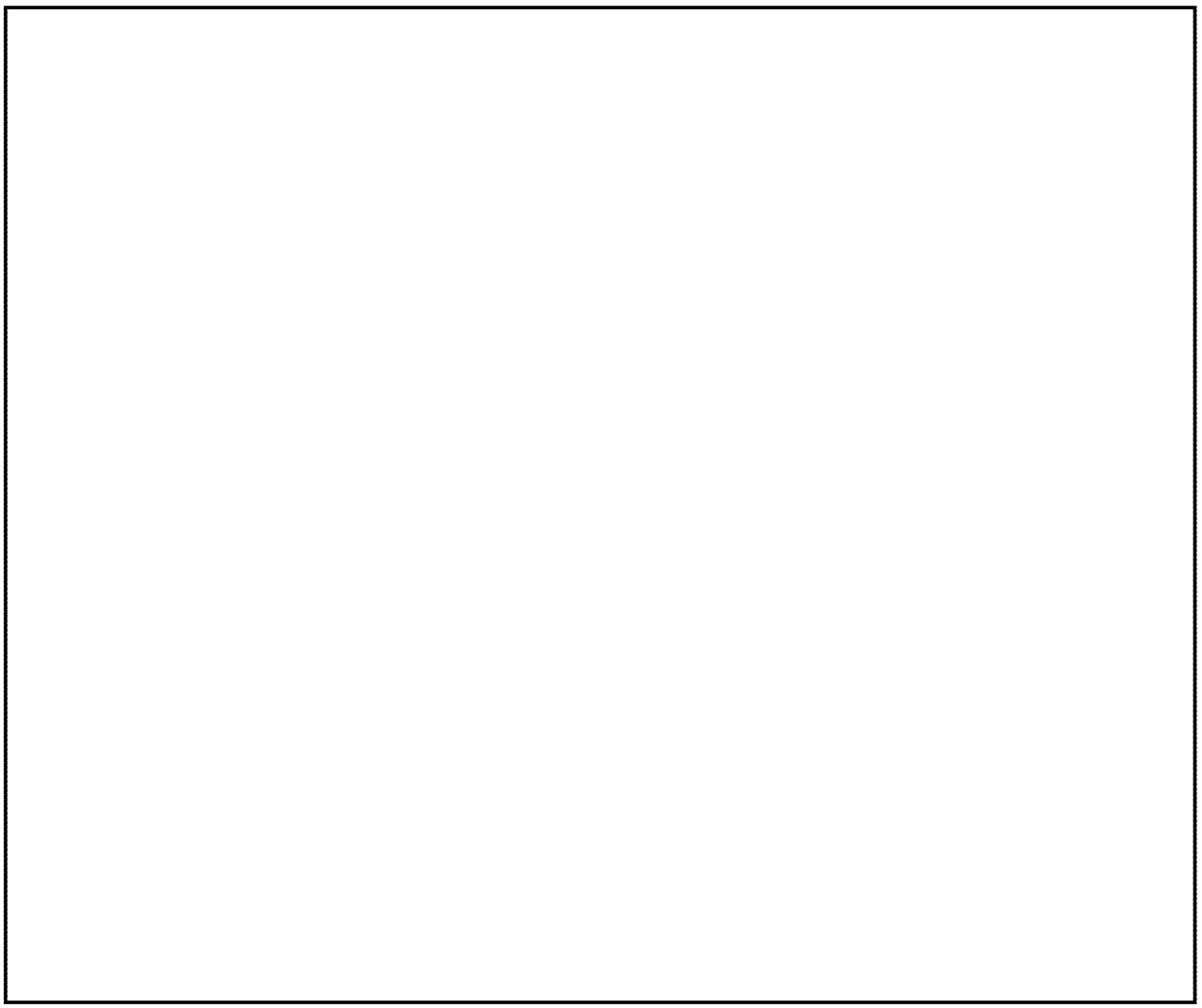
b5

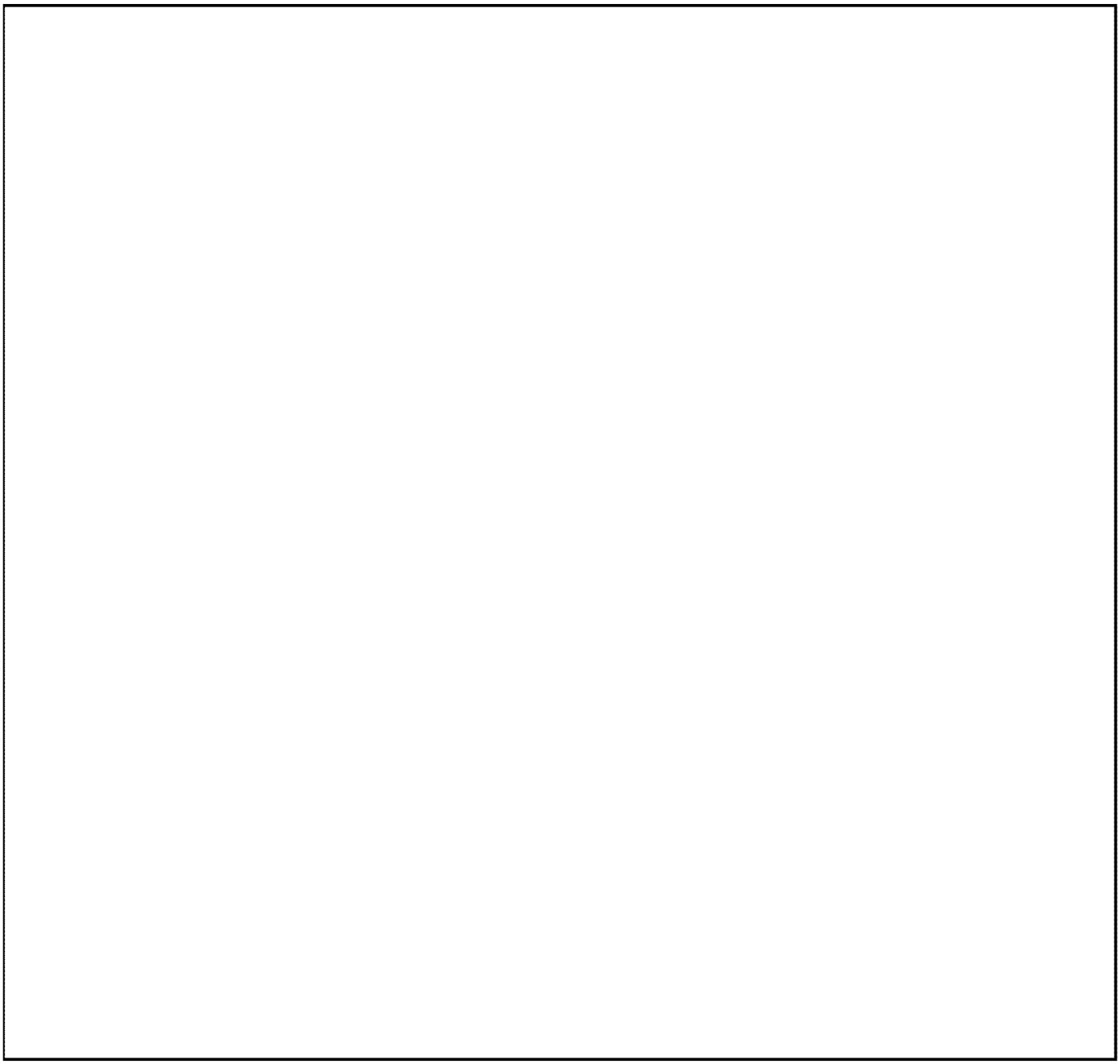
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

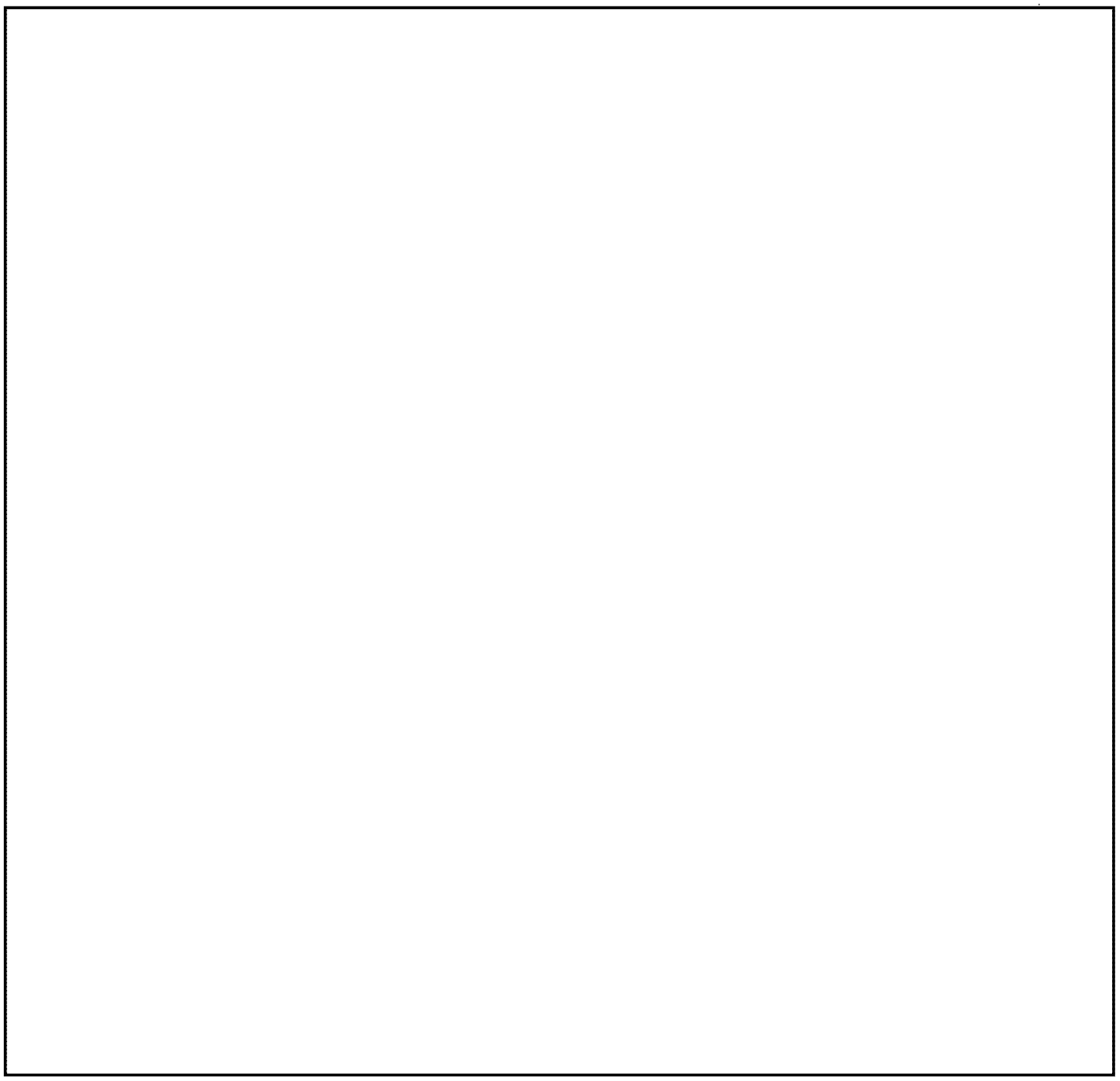
b5

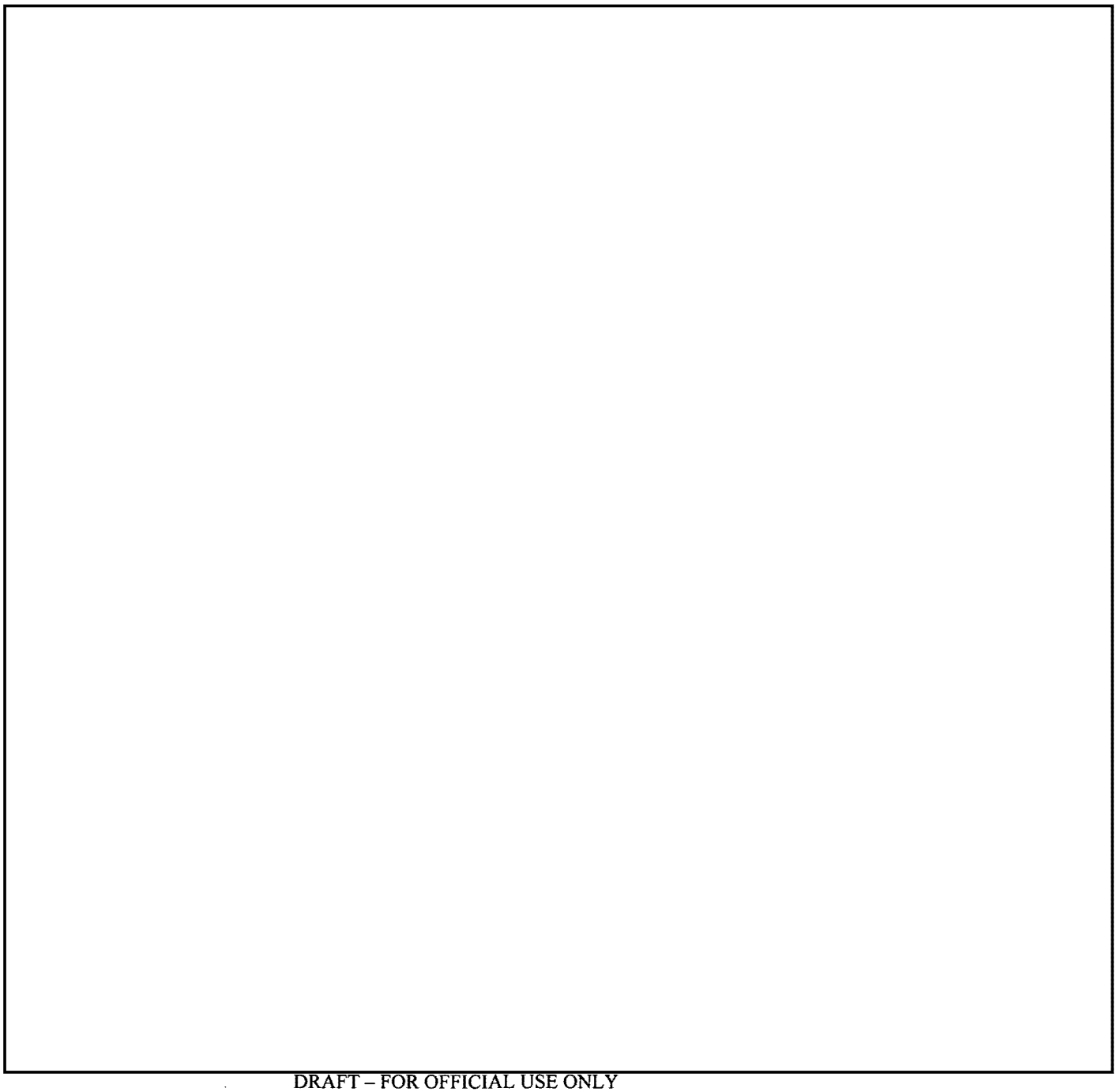
b5

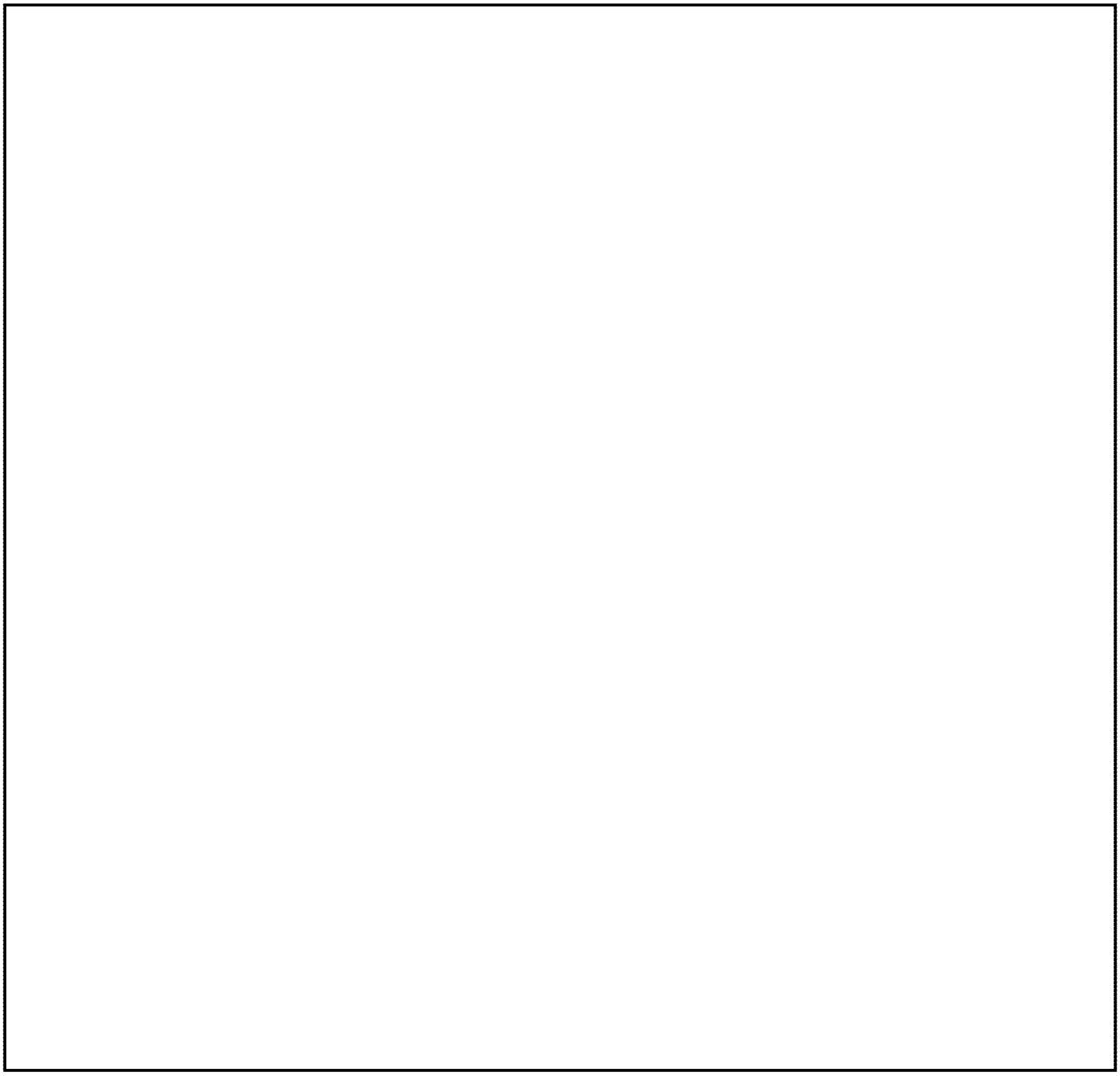
b5



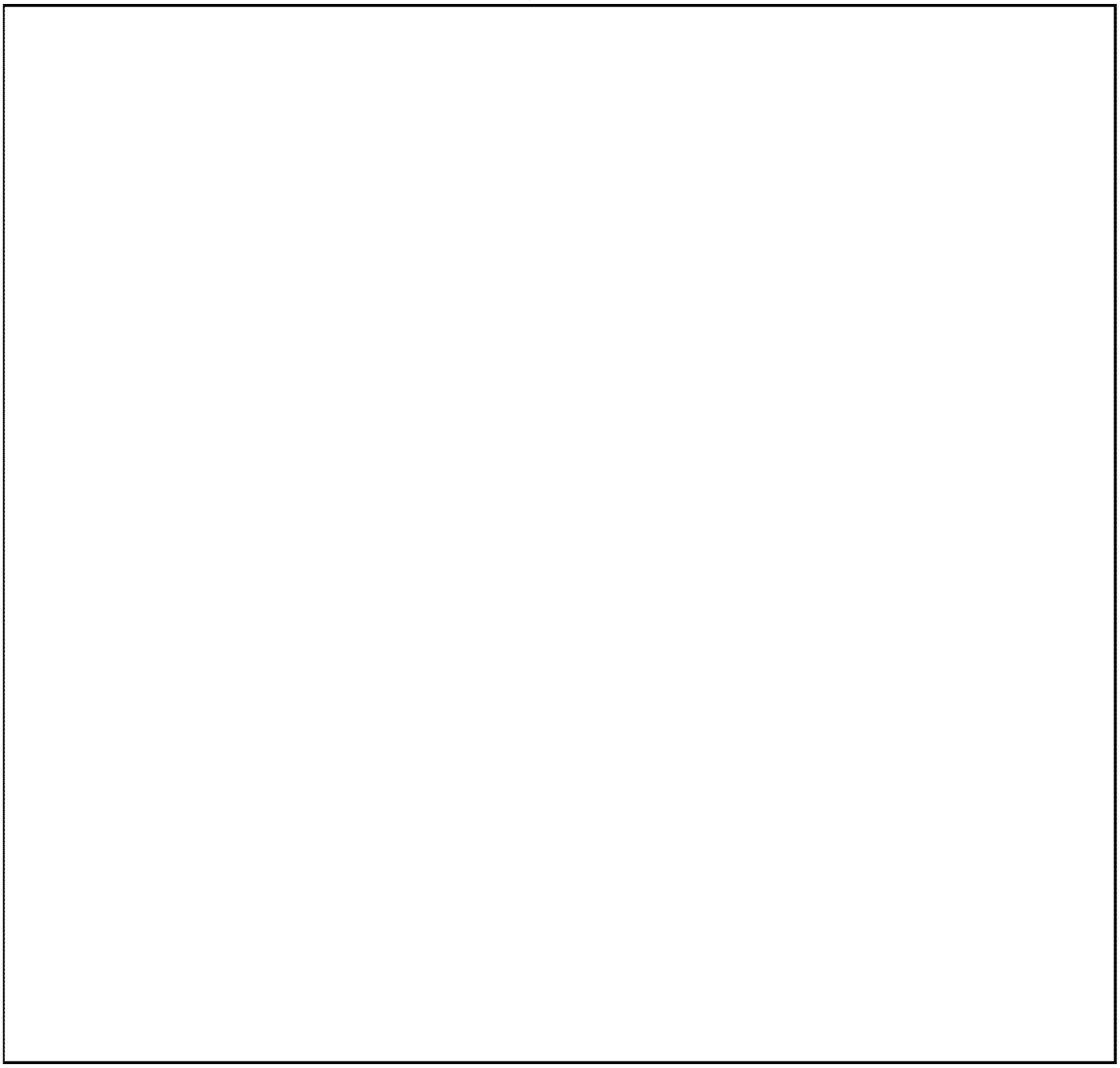


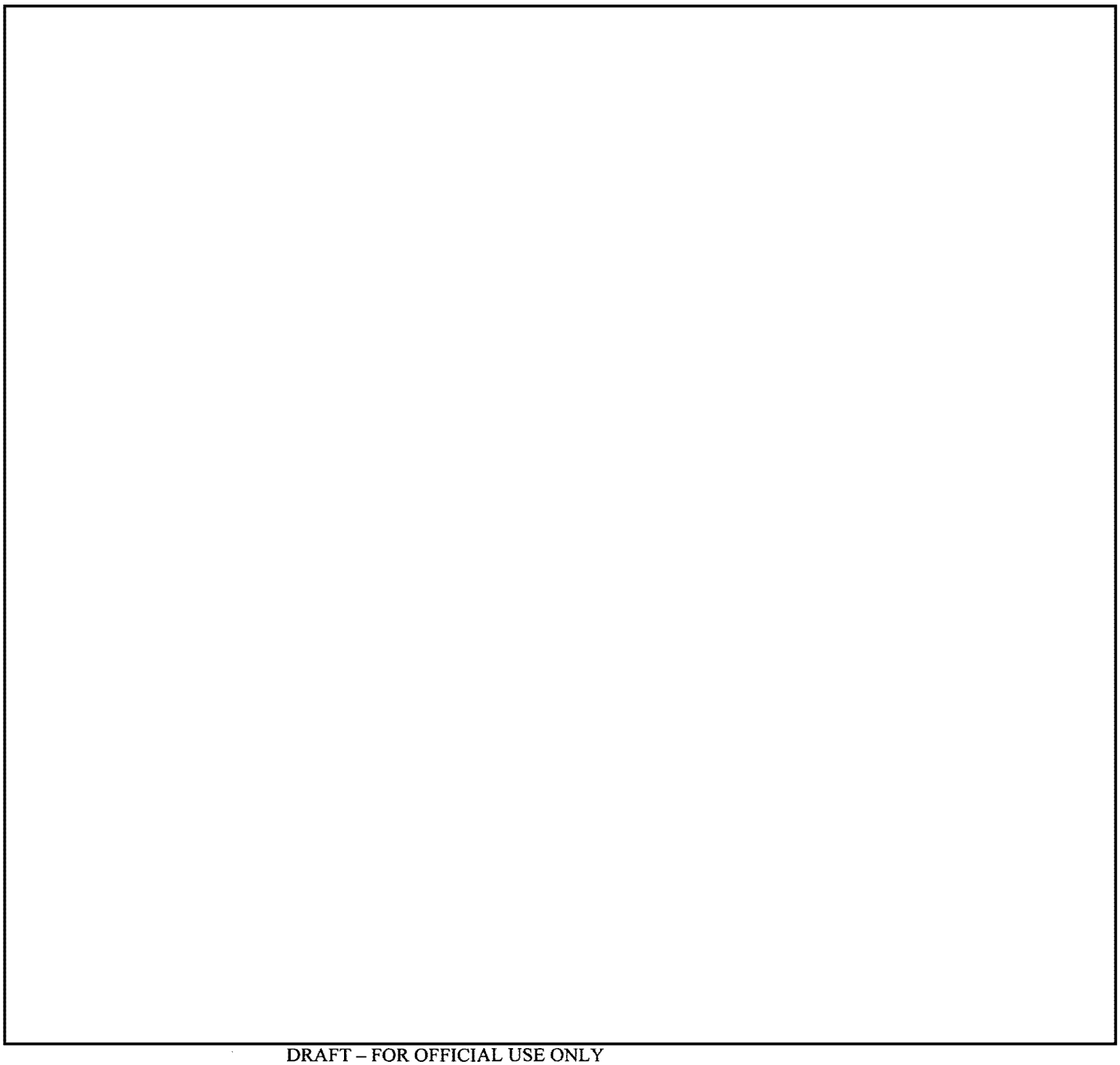




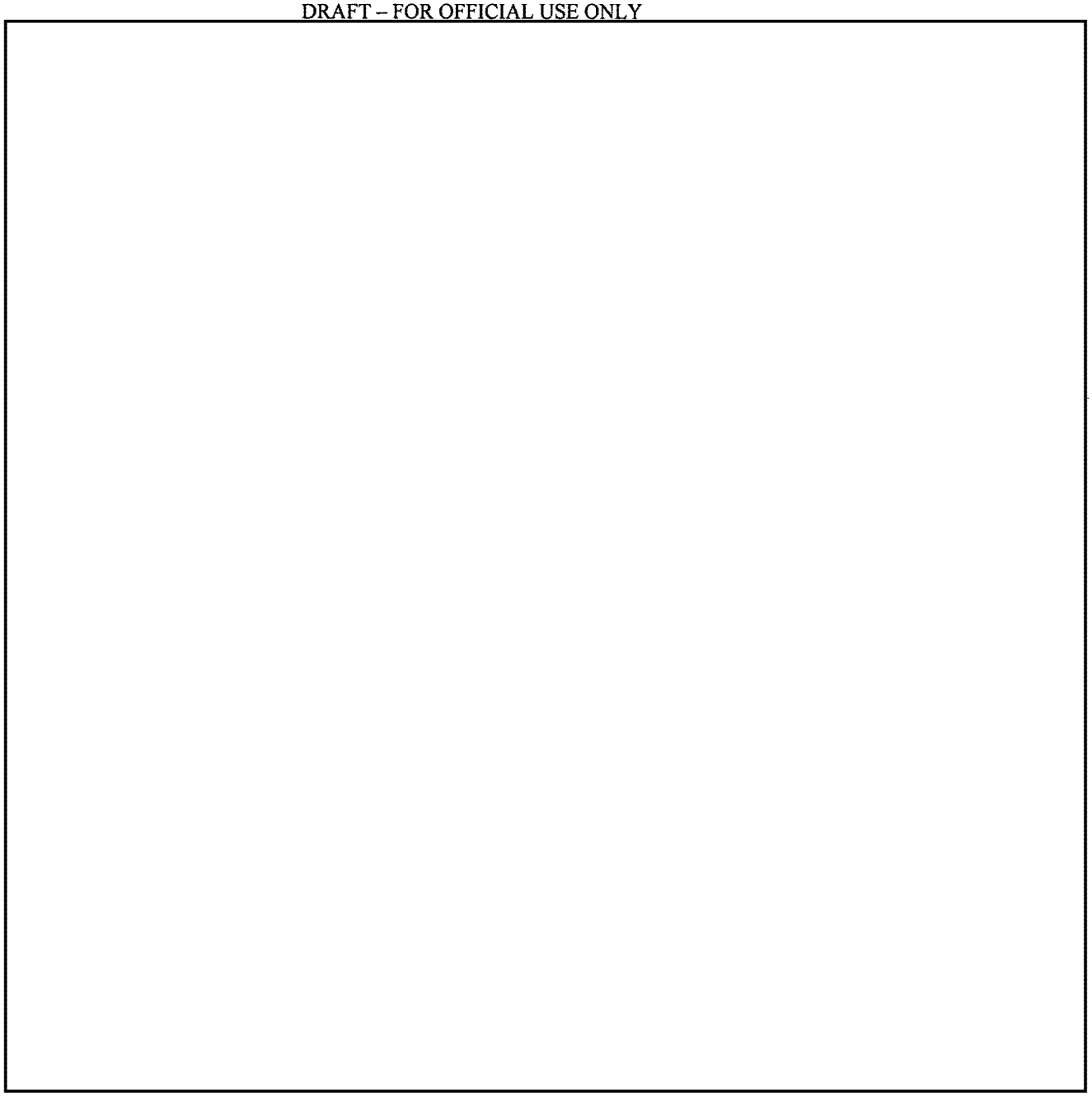


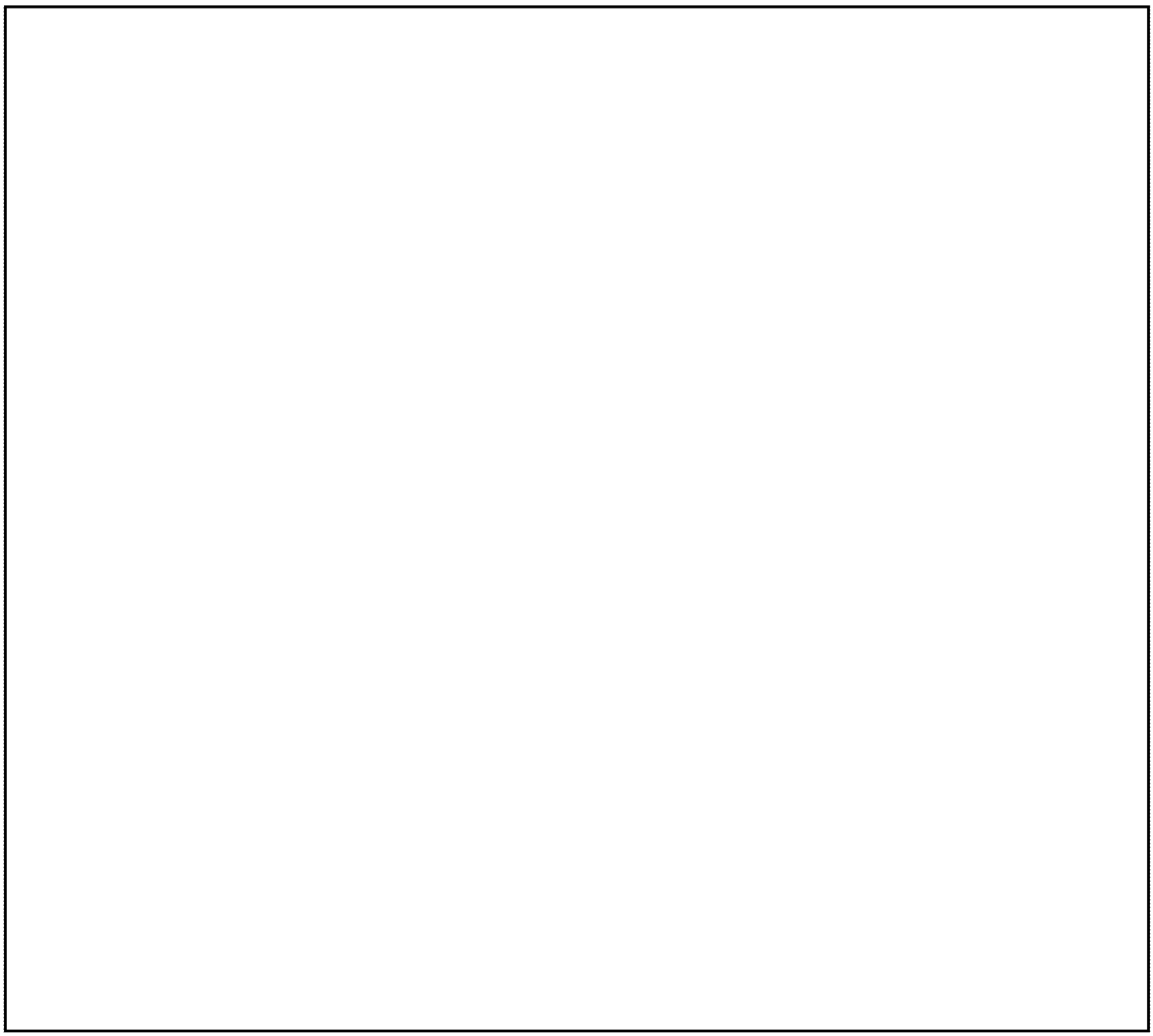
b5



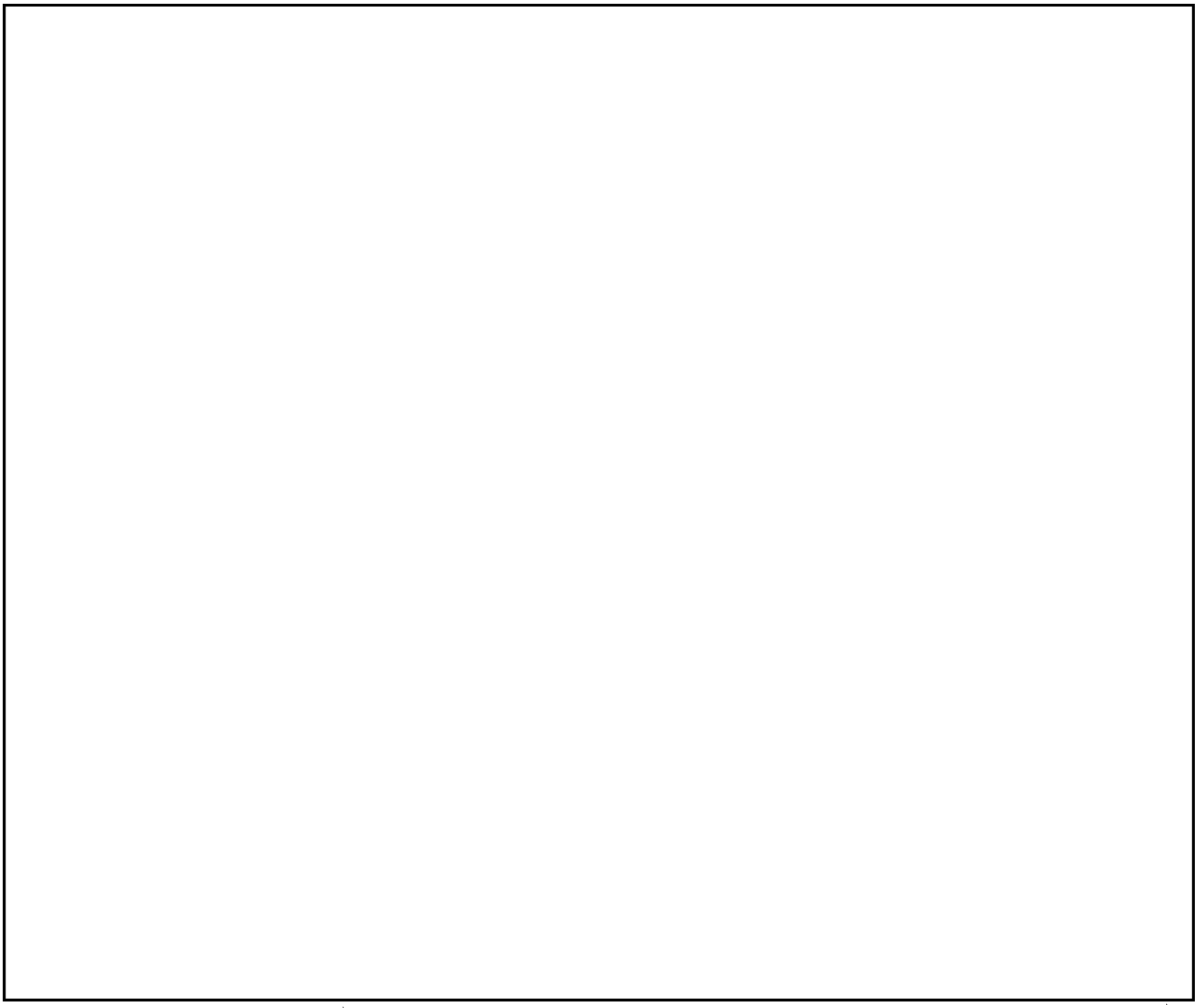


b5



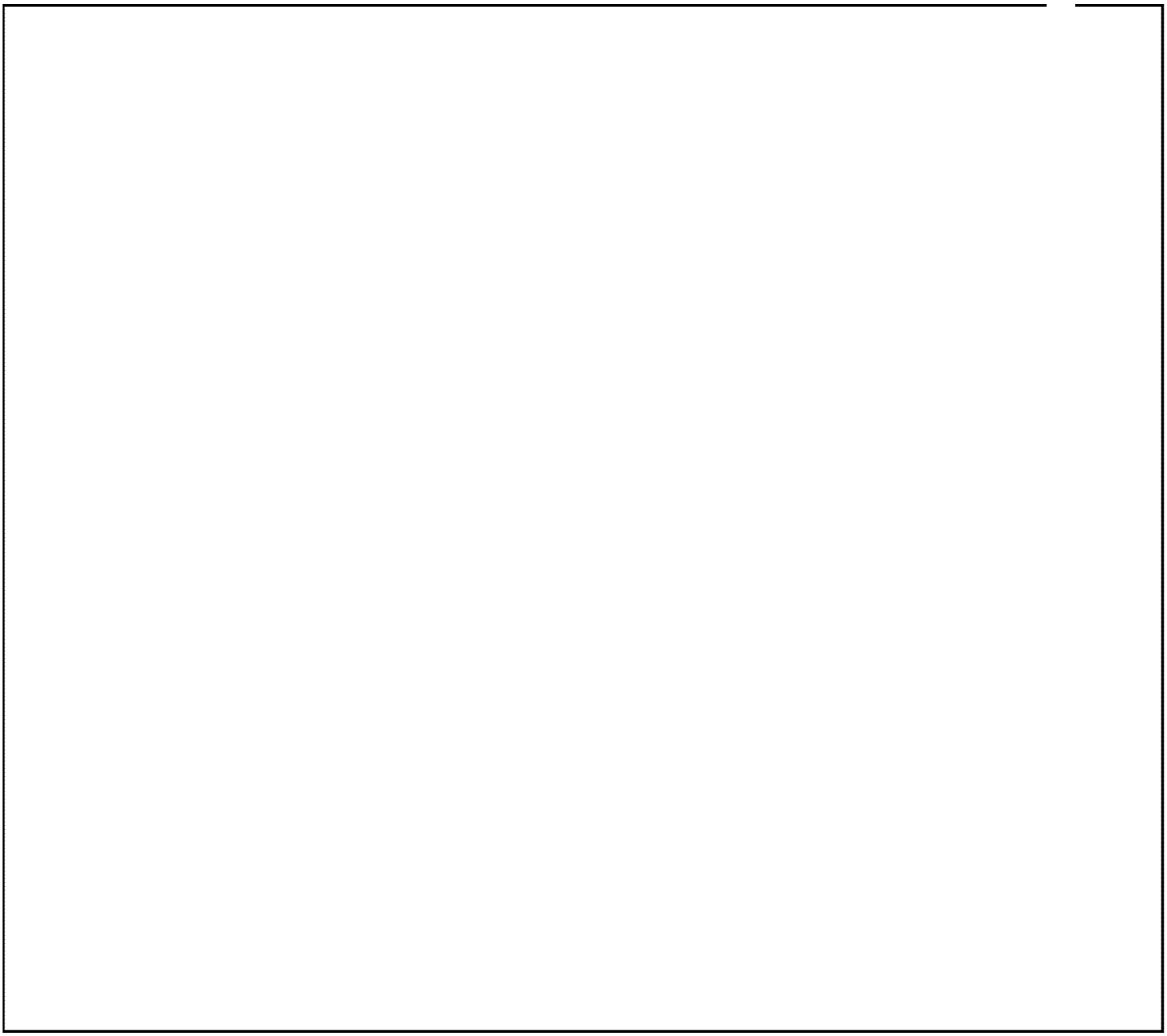


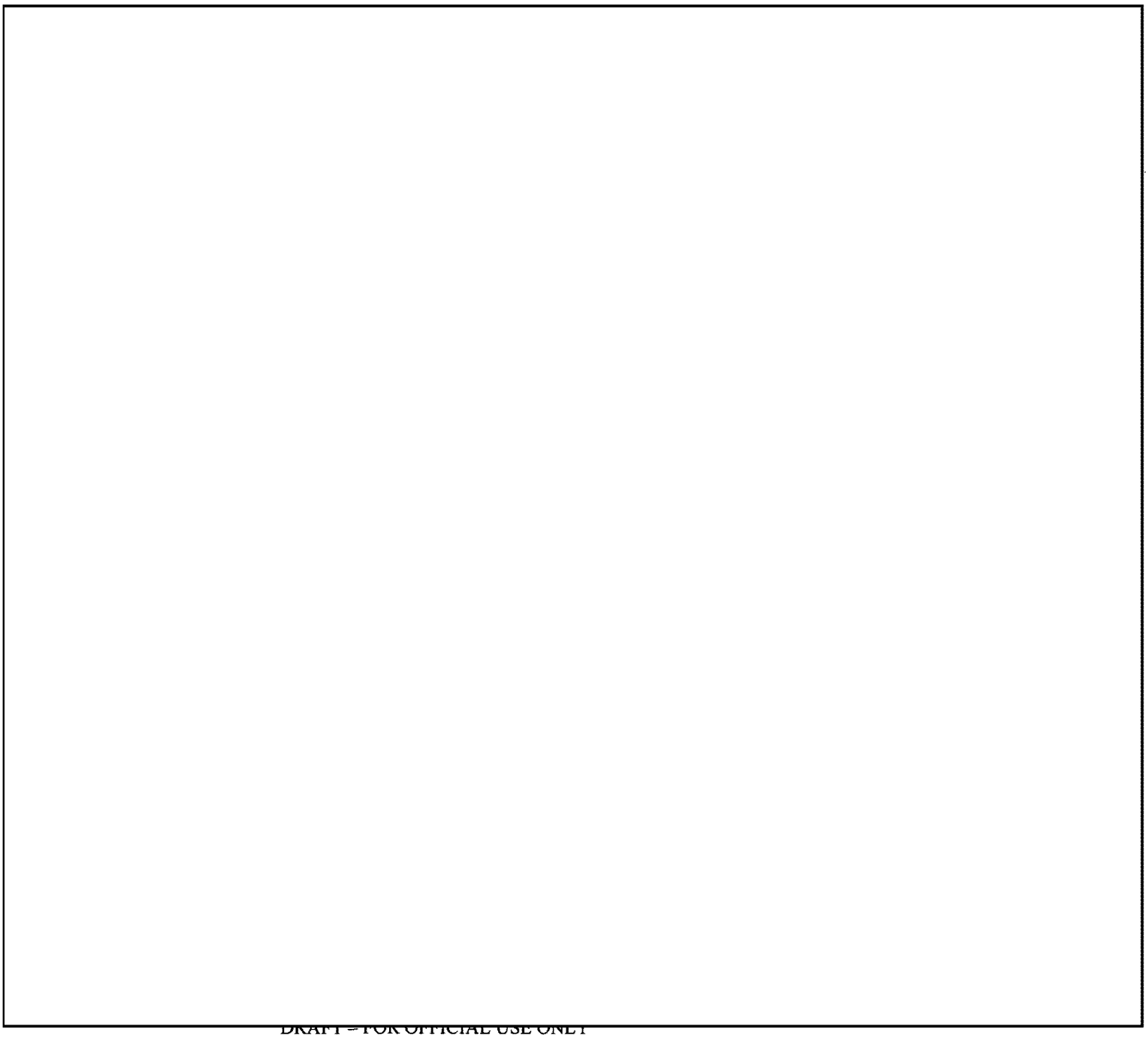
b5



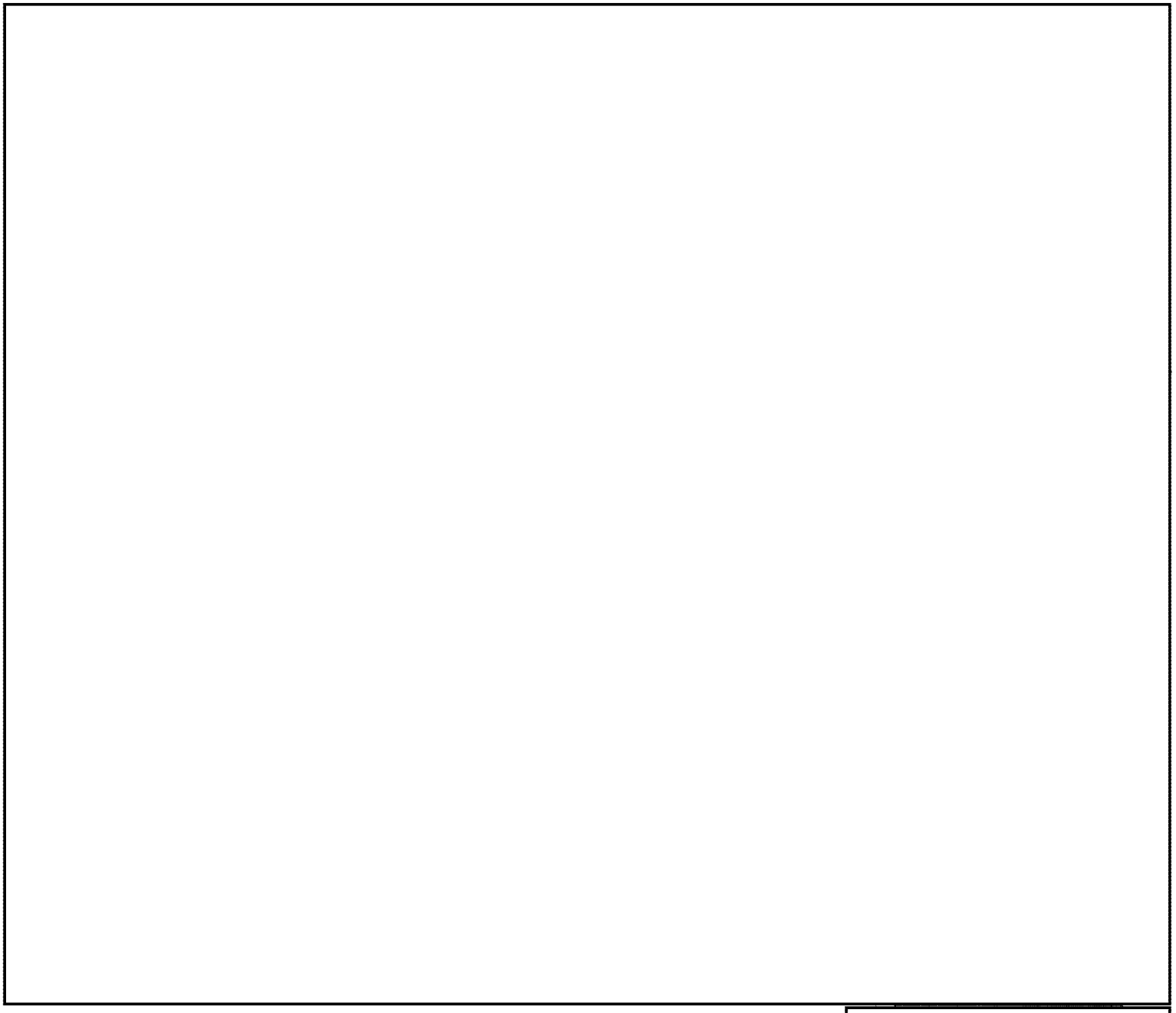
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

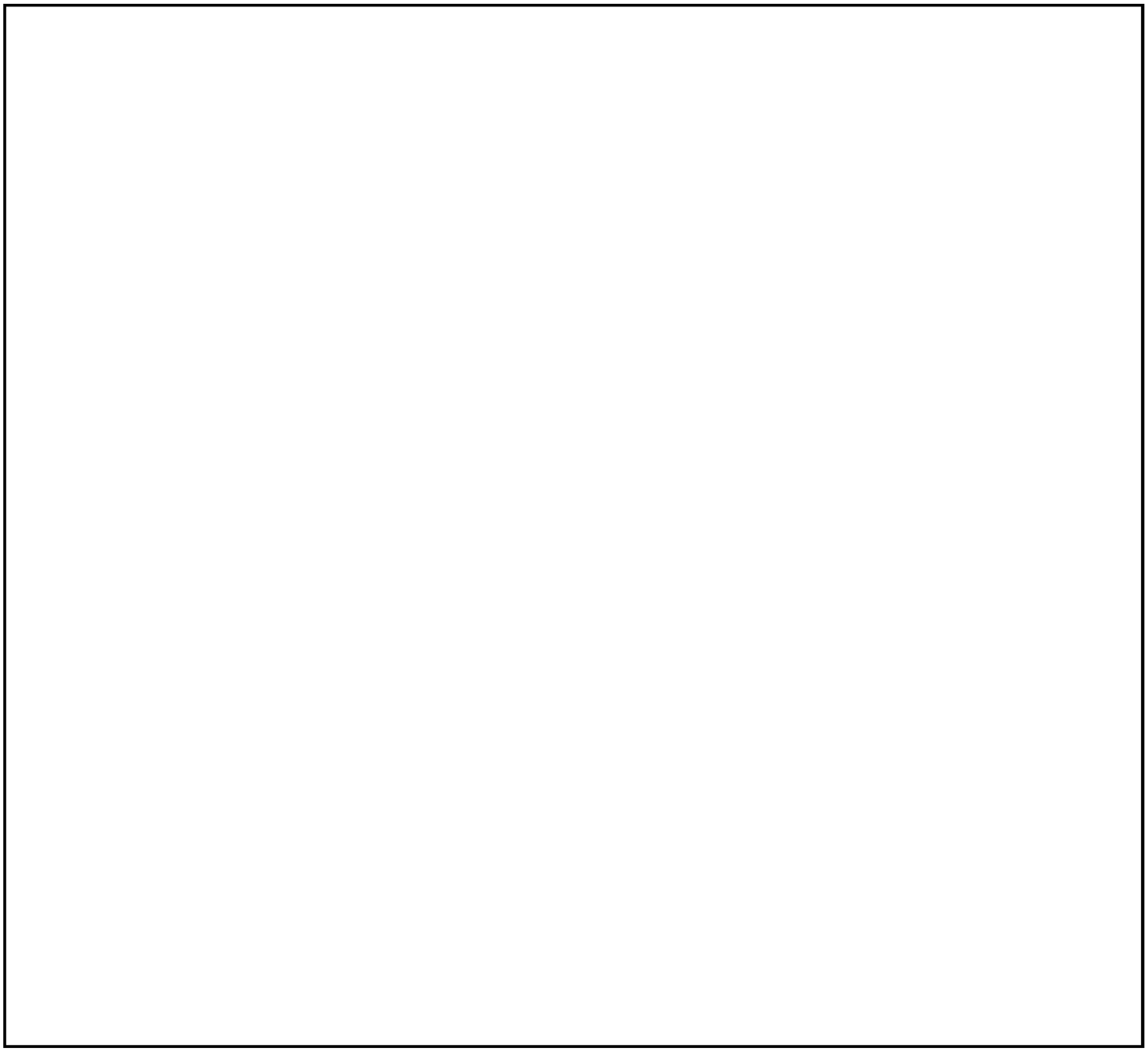
b5



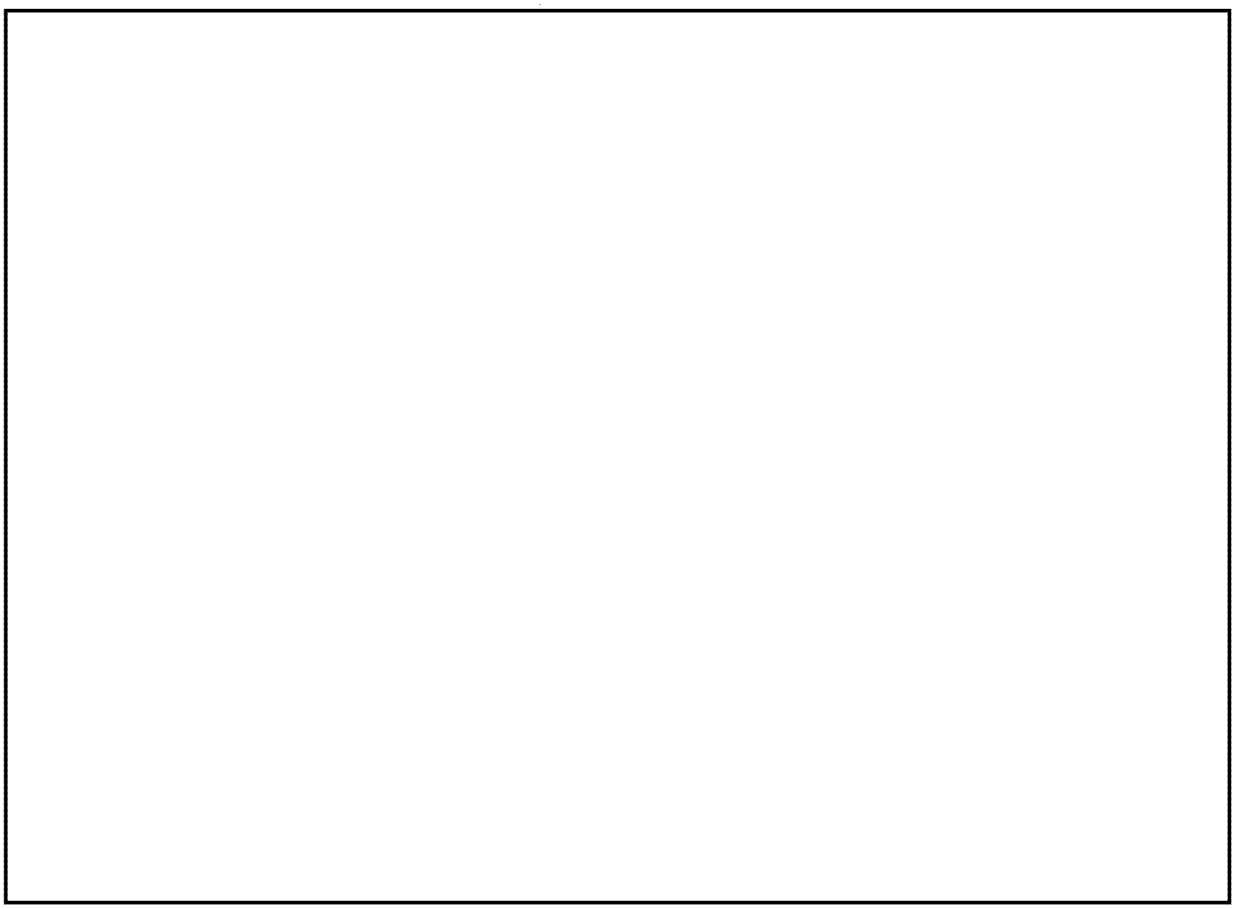


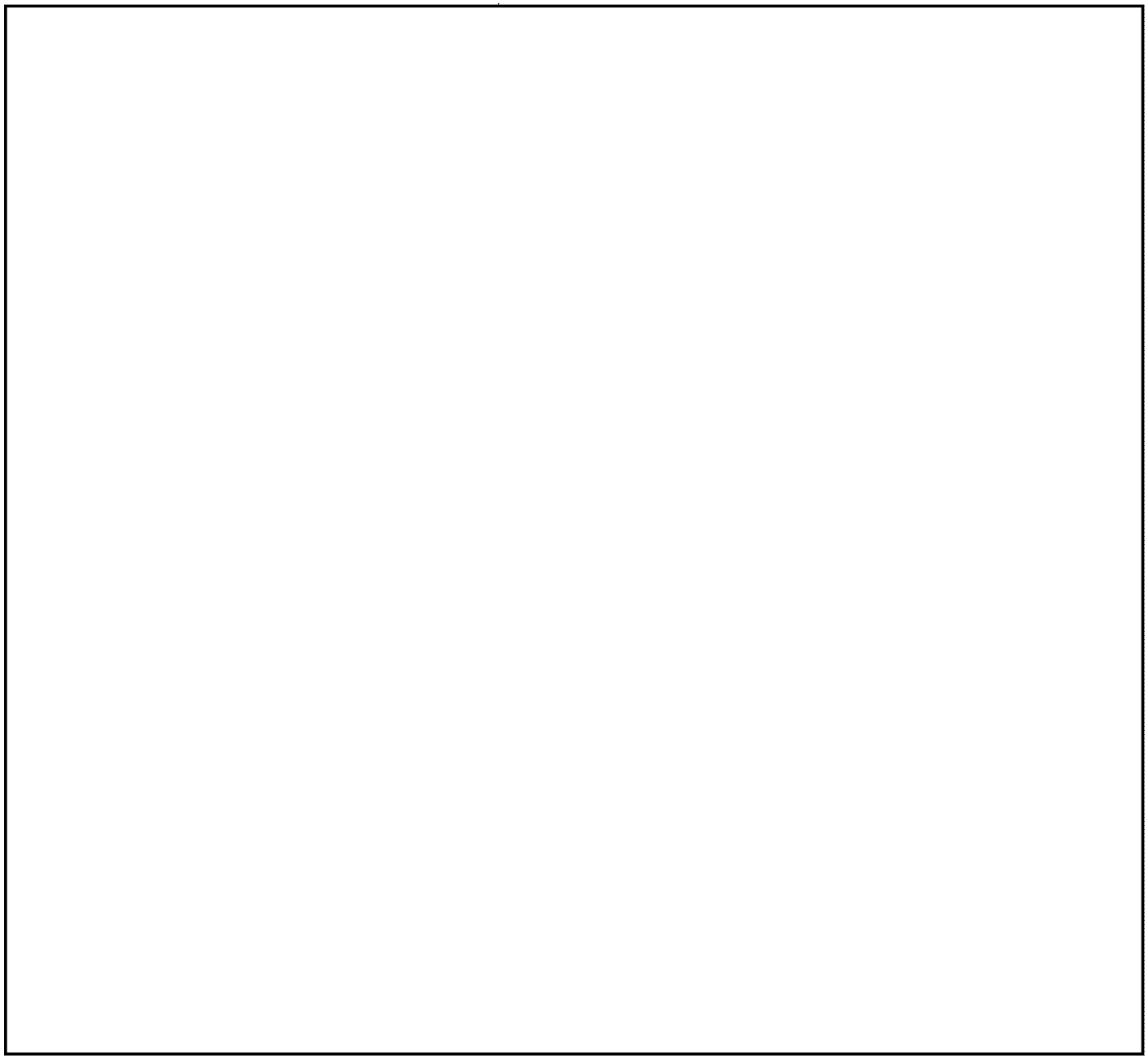
DRAFT – FOR OFFICIAL USE ONLY



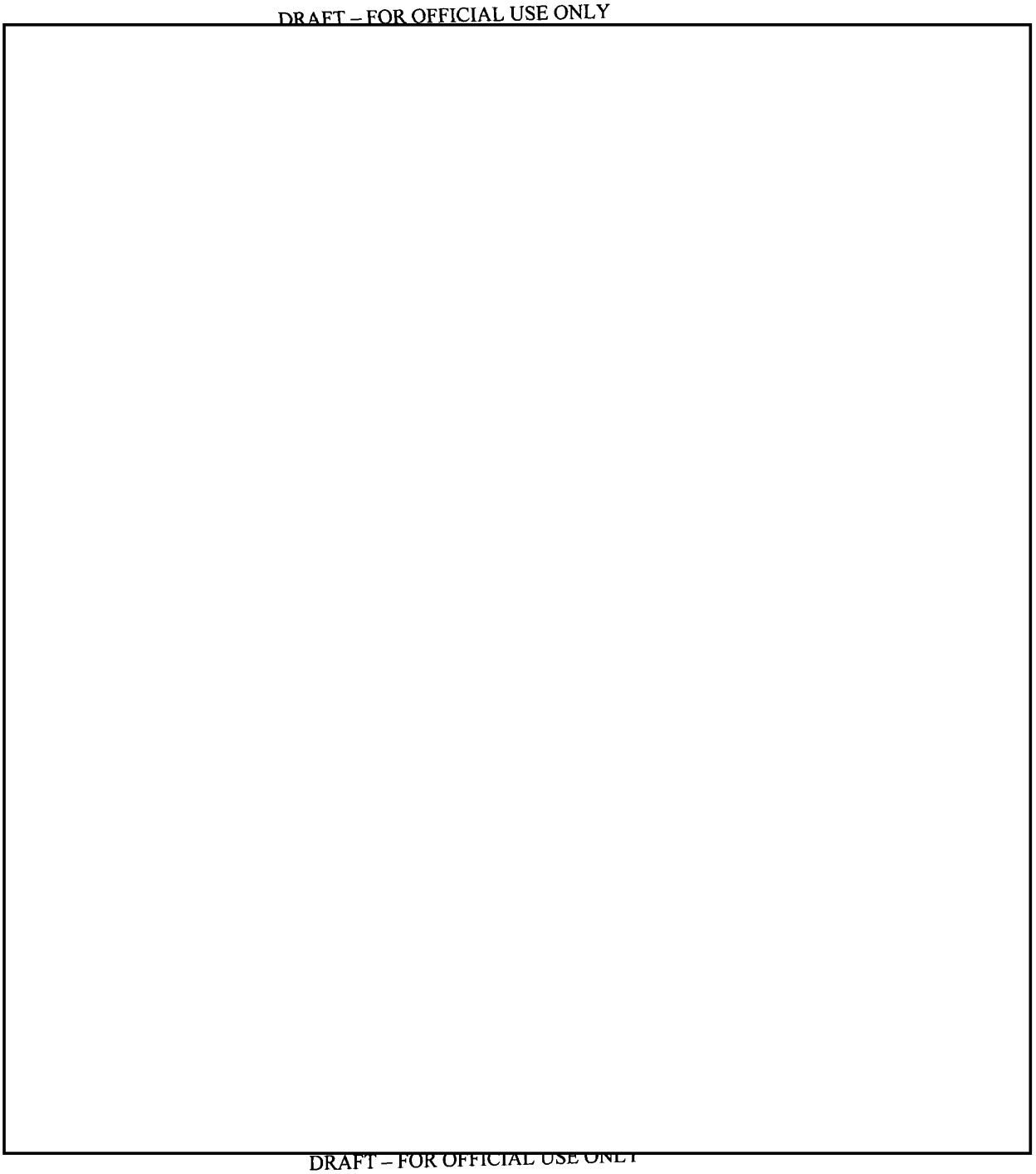


b5





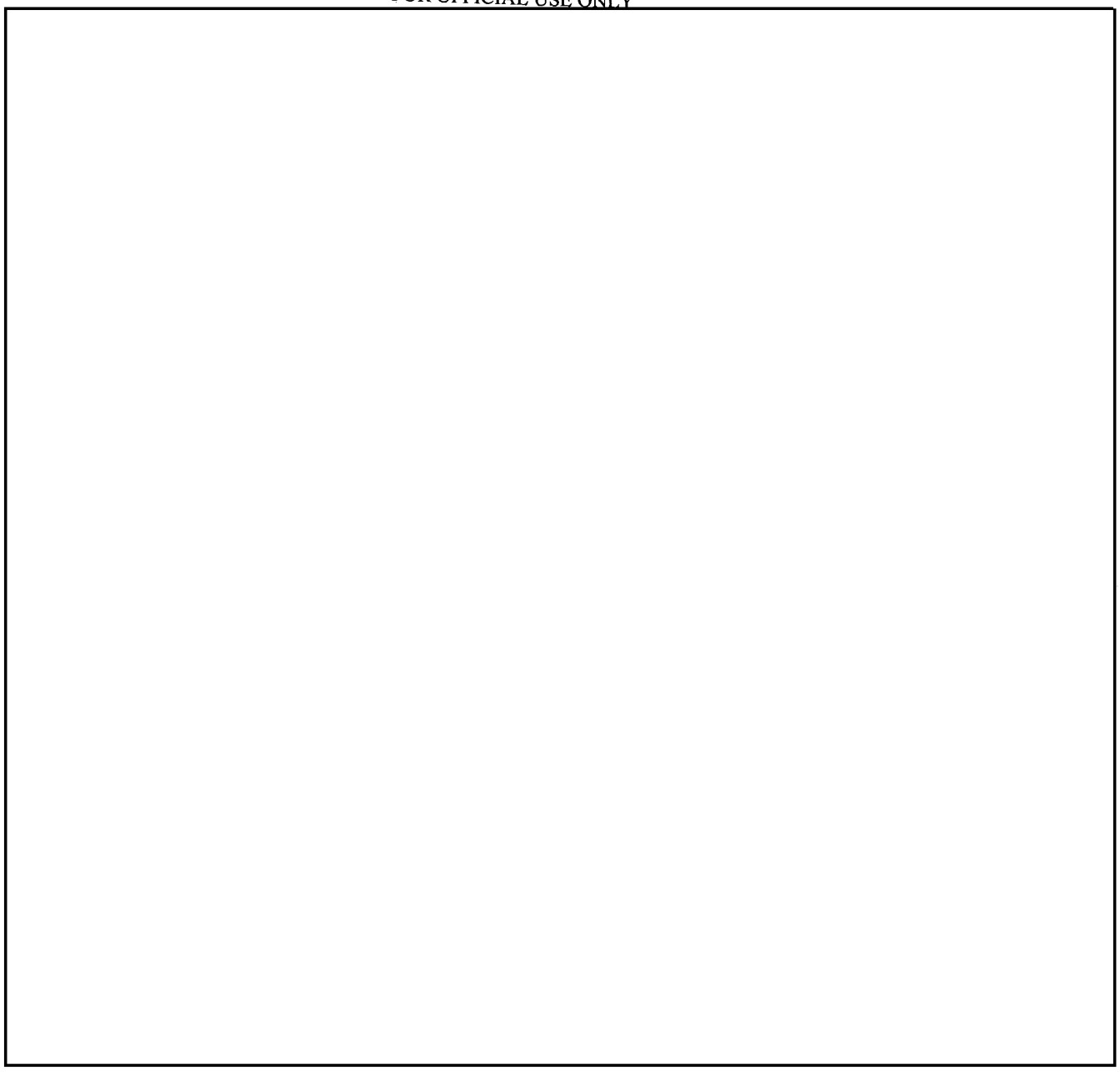
b5

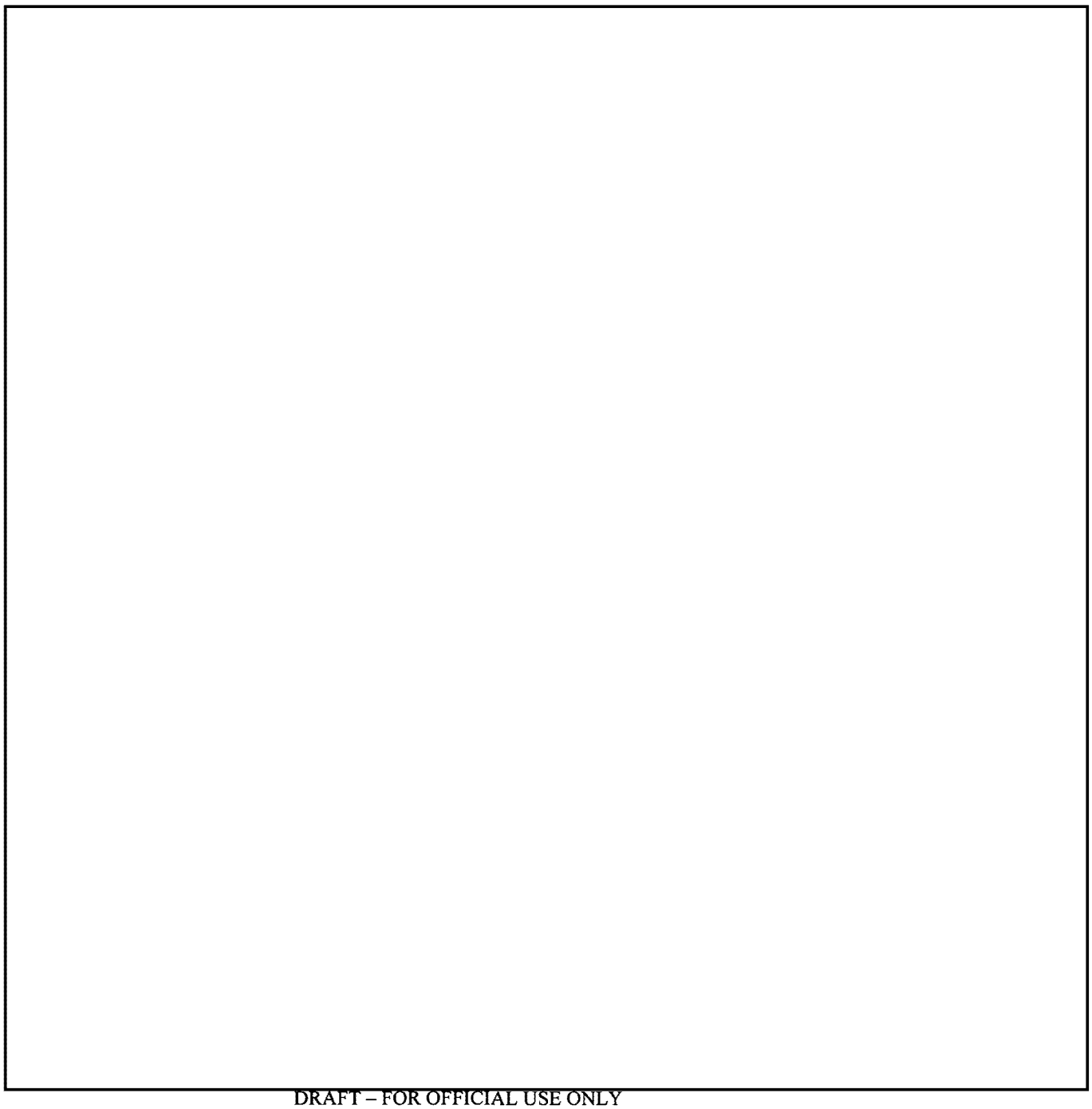


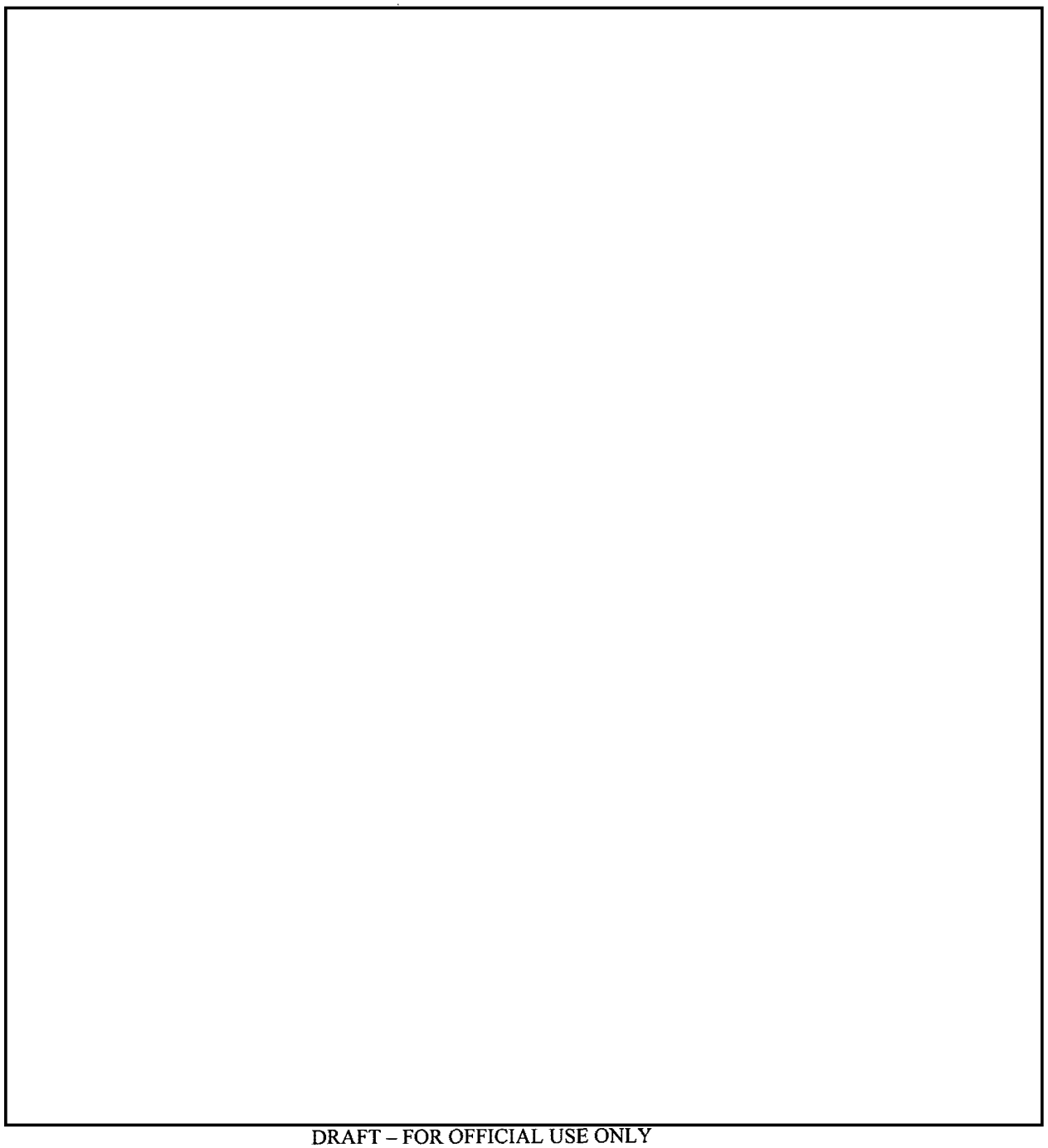
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

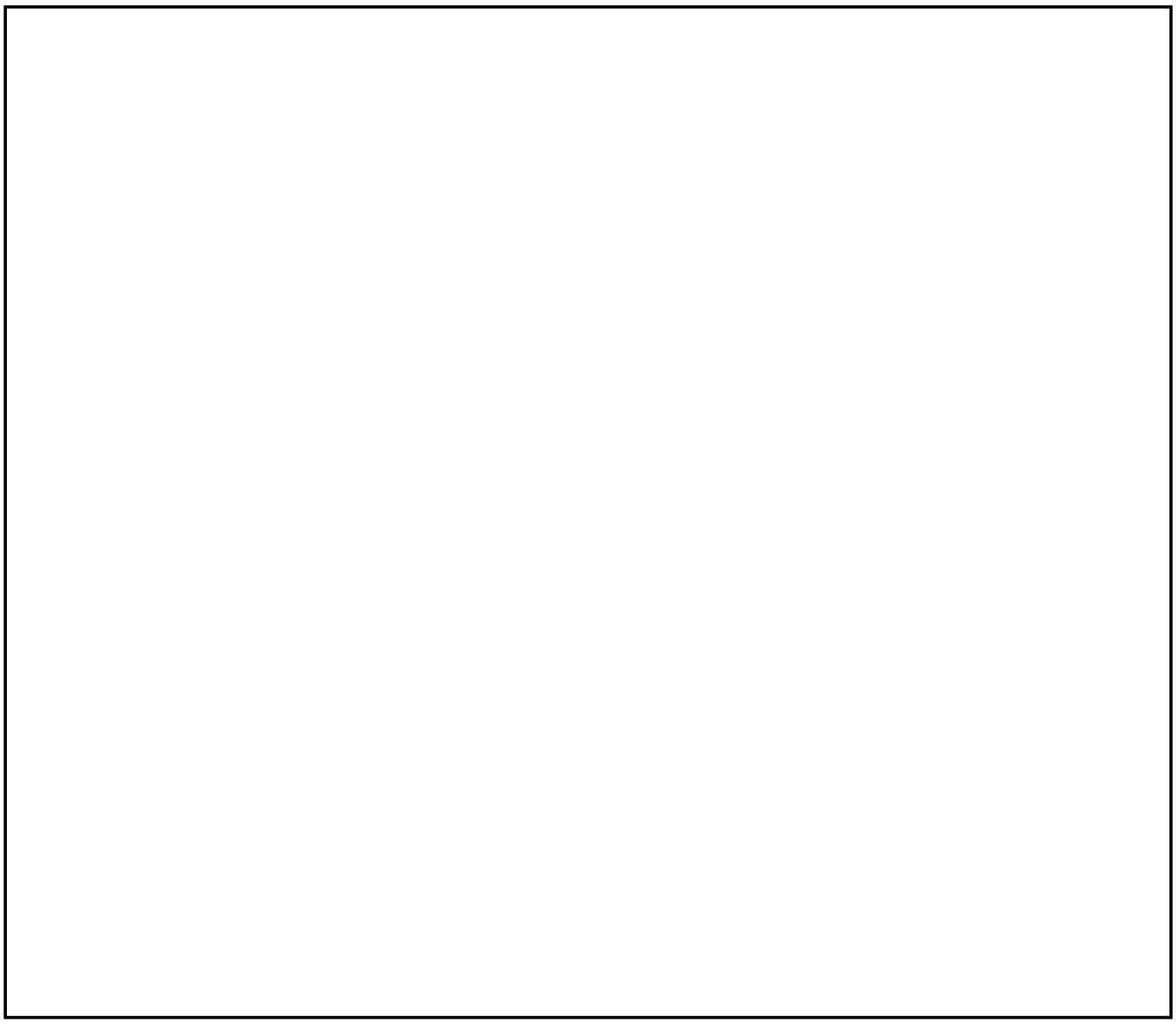




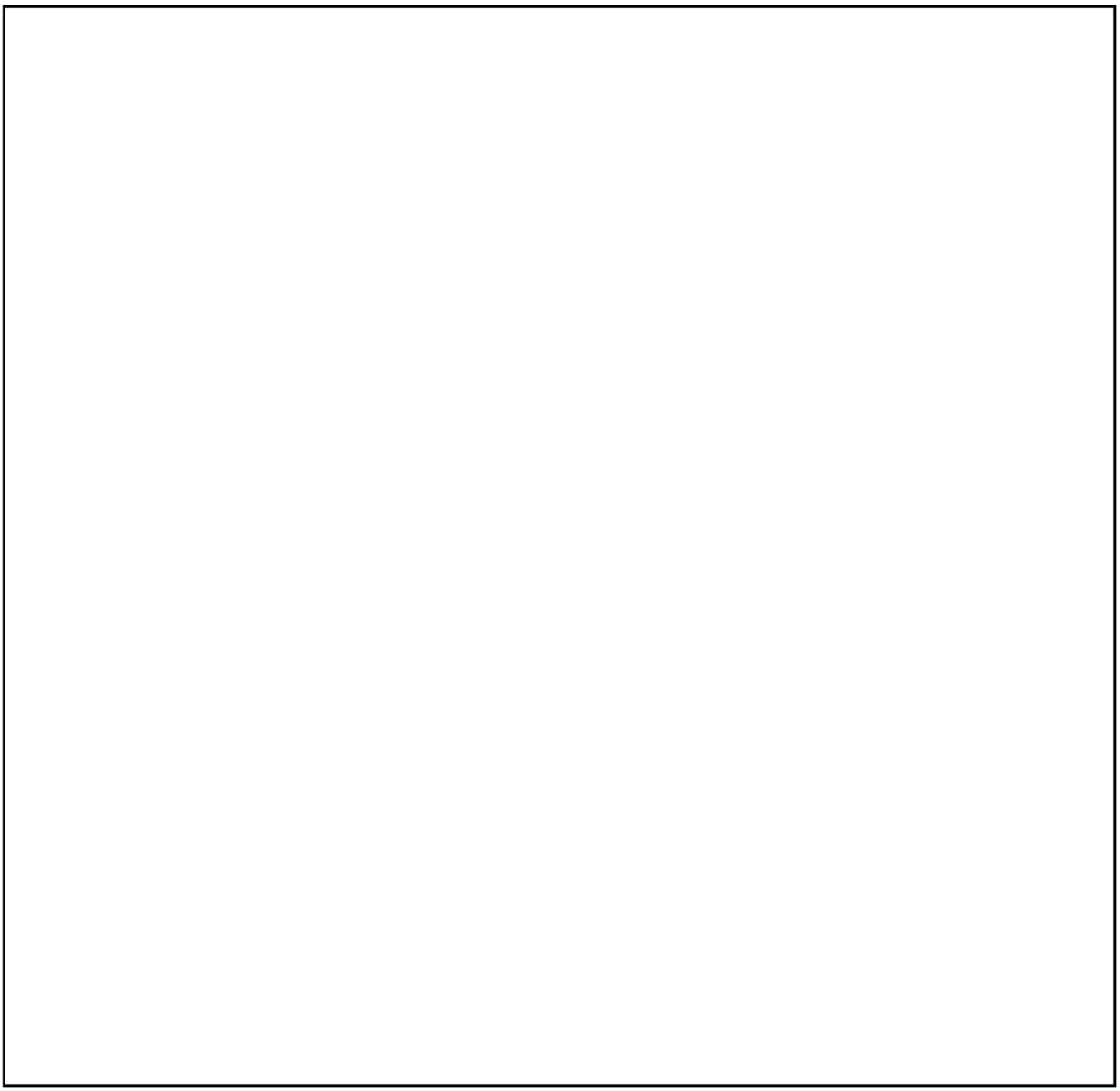


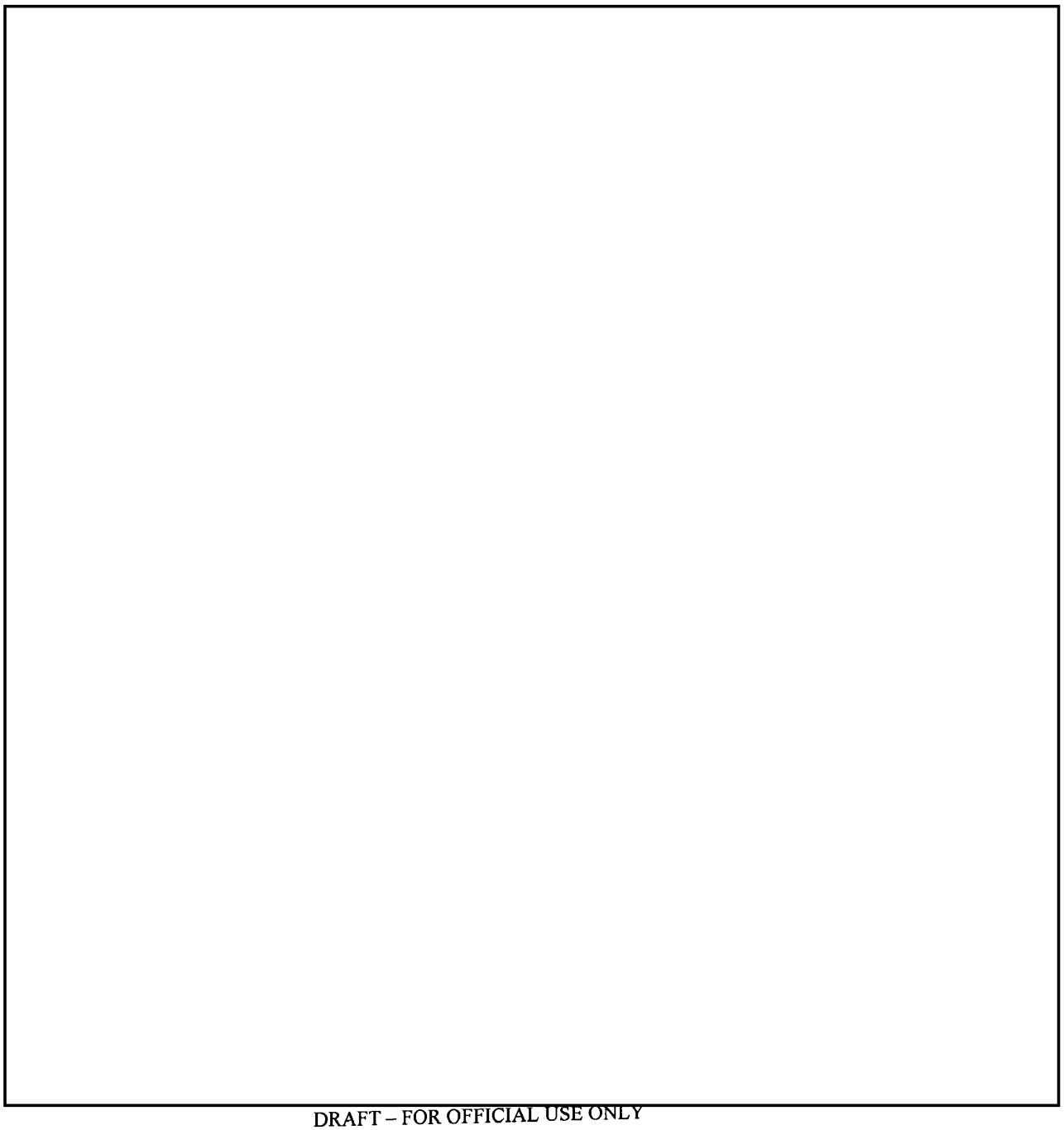
b5

b5

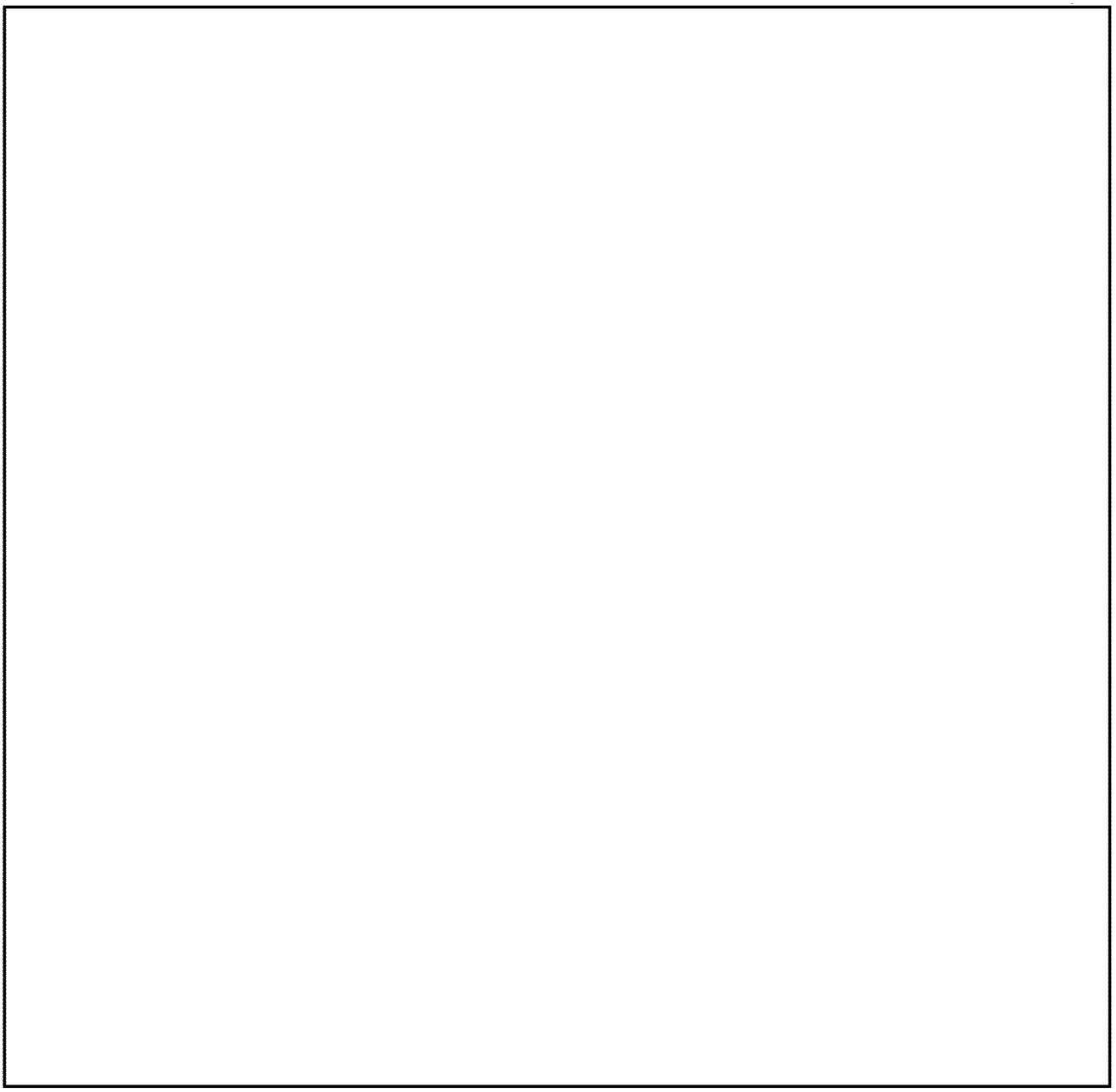


b5

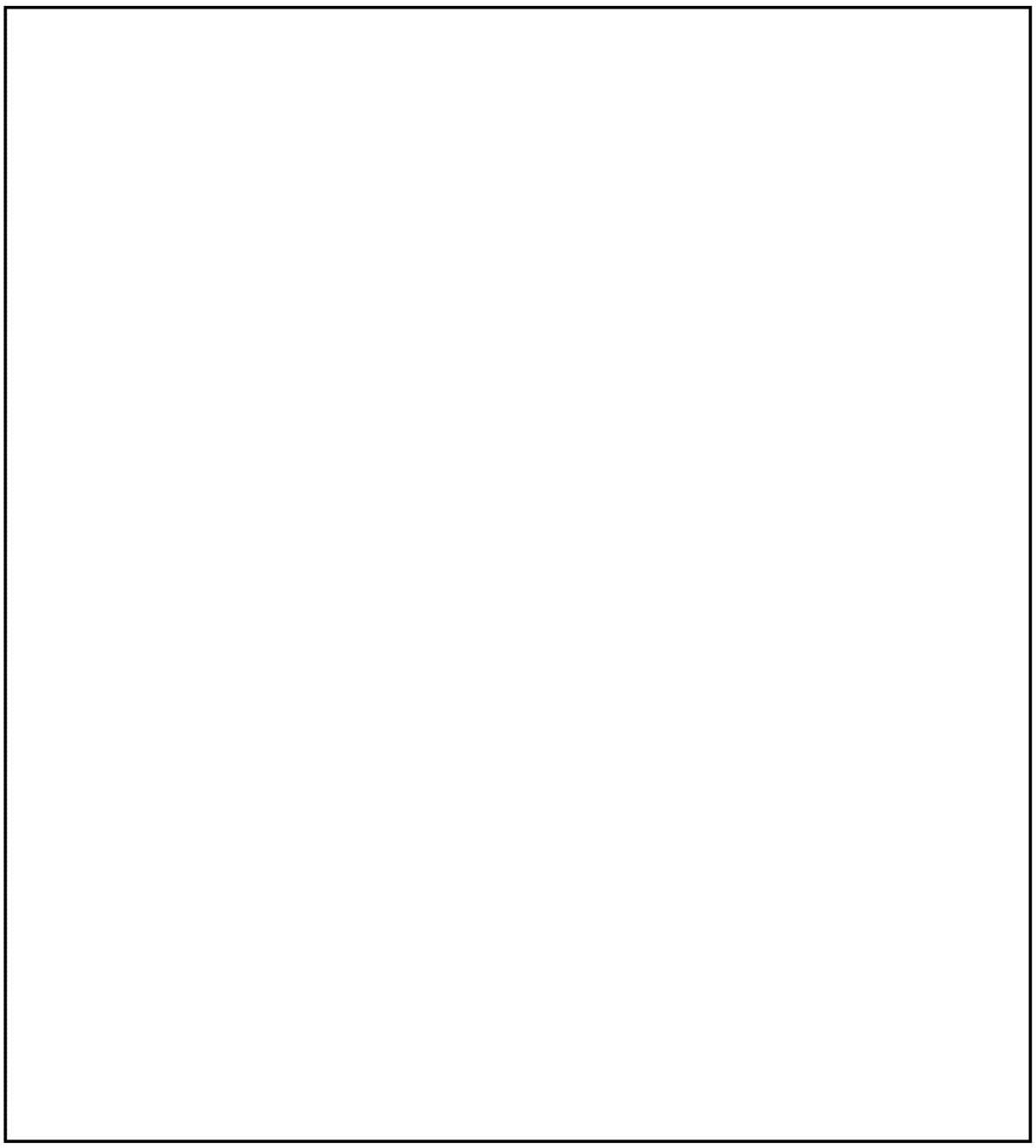




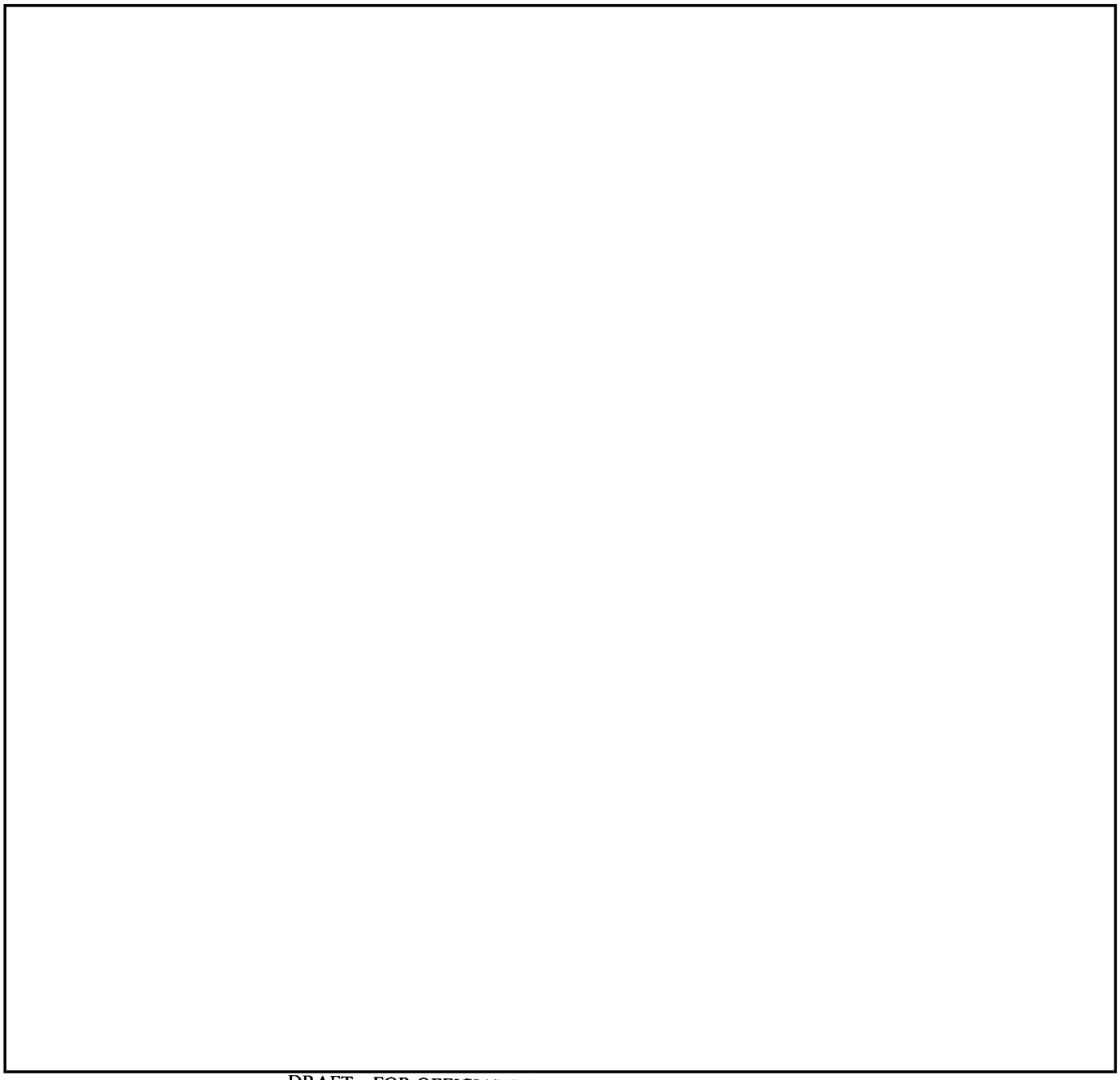
b5



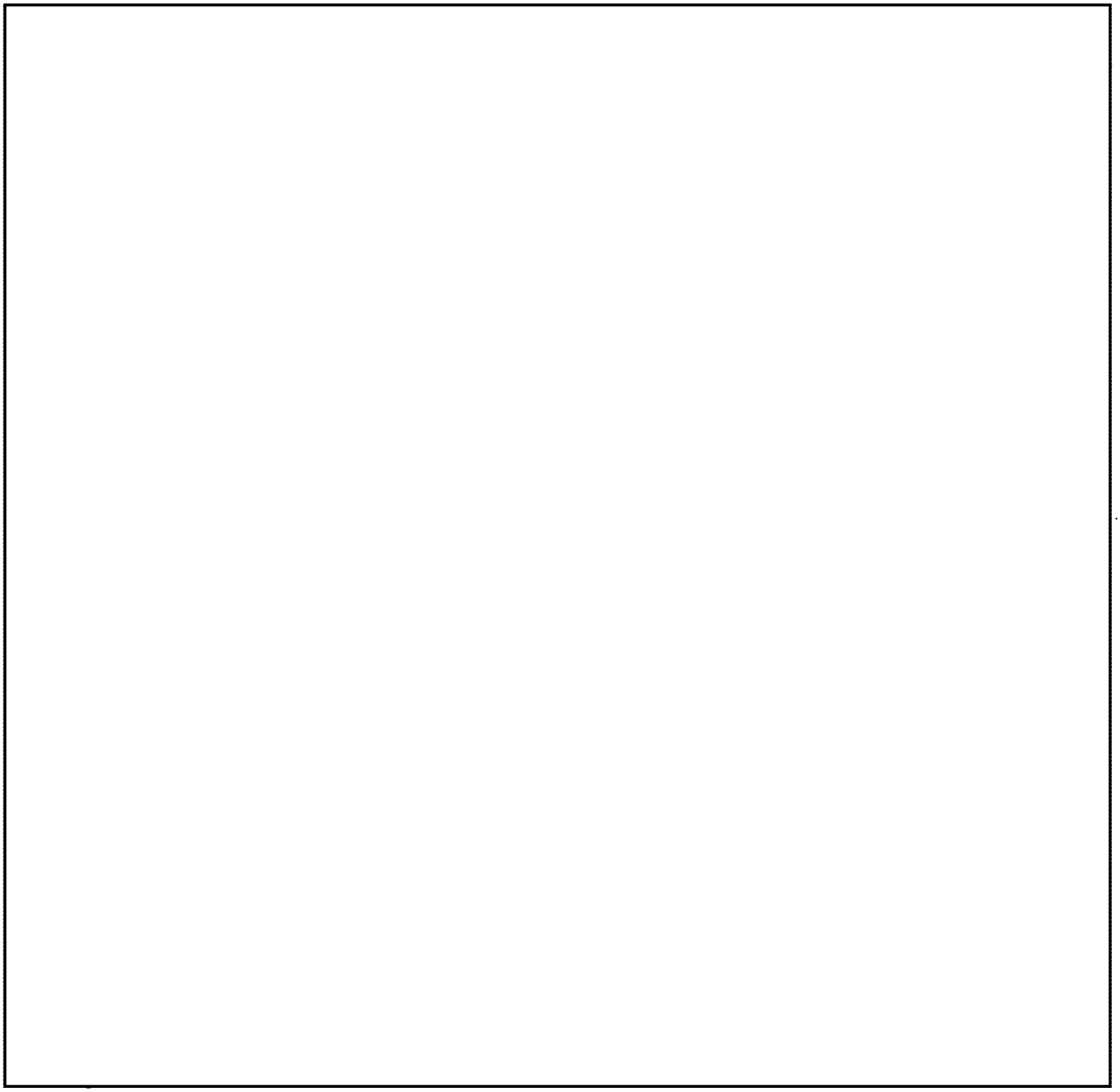
b5

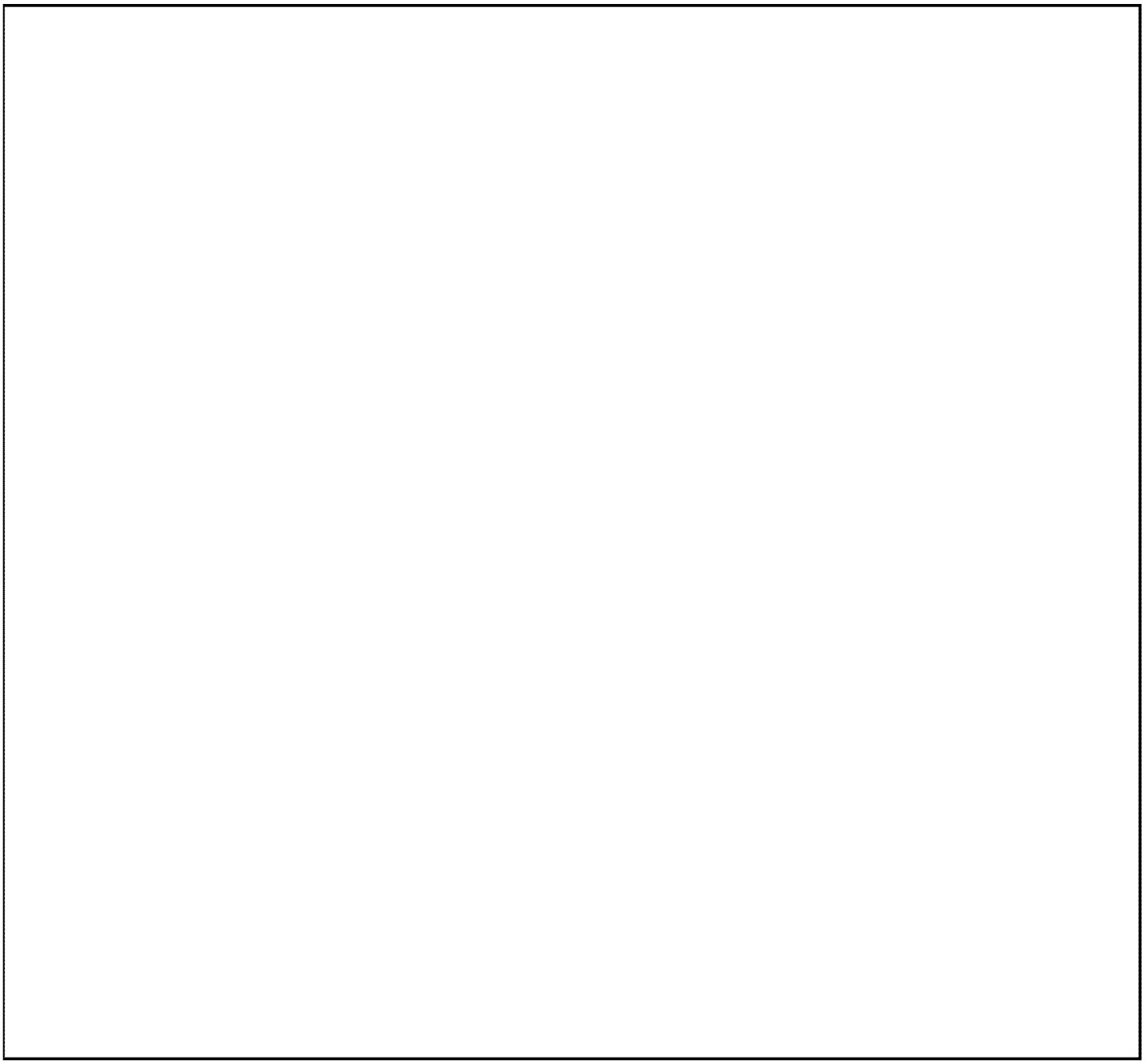


b5



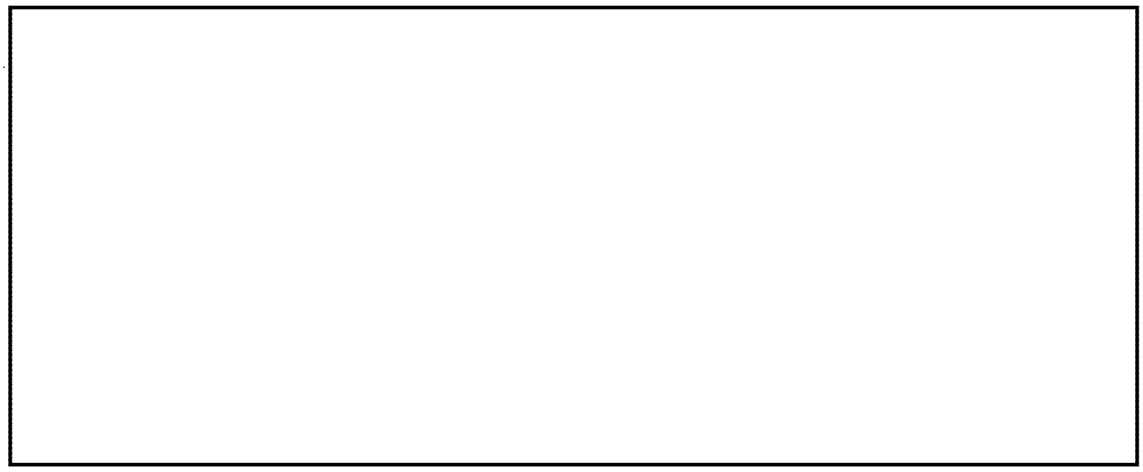
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT





PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



b5

b6
b7C

RE Intel Manual.txt

MessageFrom: [redacted] (OGC) (FBI)
Sent: Monday, August 23, 2004 8:44 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: RE: Intel Manual

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b5

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, August 19, 2004 6:25 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); KELLEY, PATRICK W. (OGC) (FBI)

b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

Subject: RE: Intel Manual

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, August 19, 2004 5:55 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); [redacted] (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: RE: Intel Manual

b6
b7C

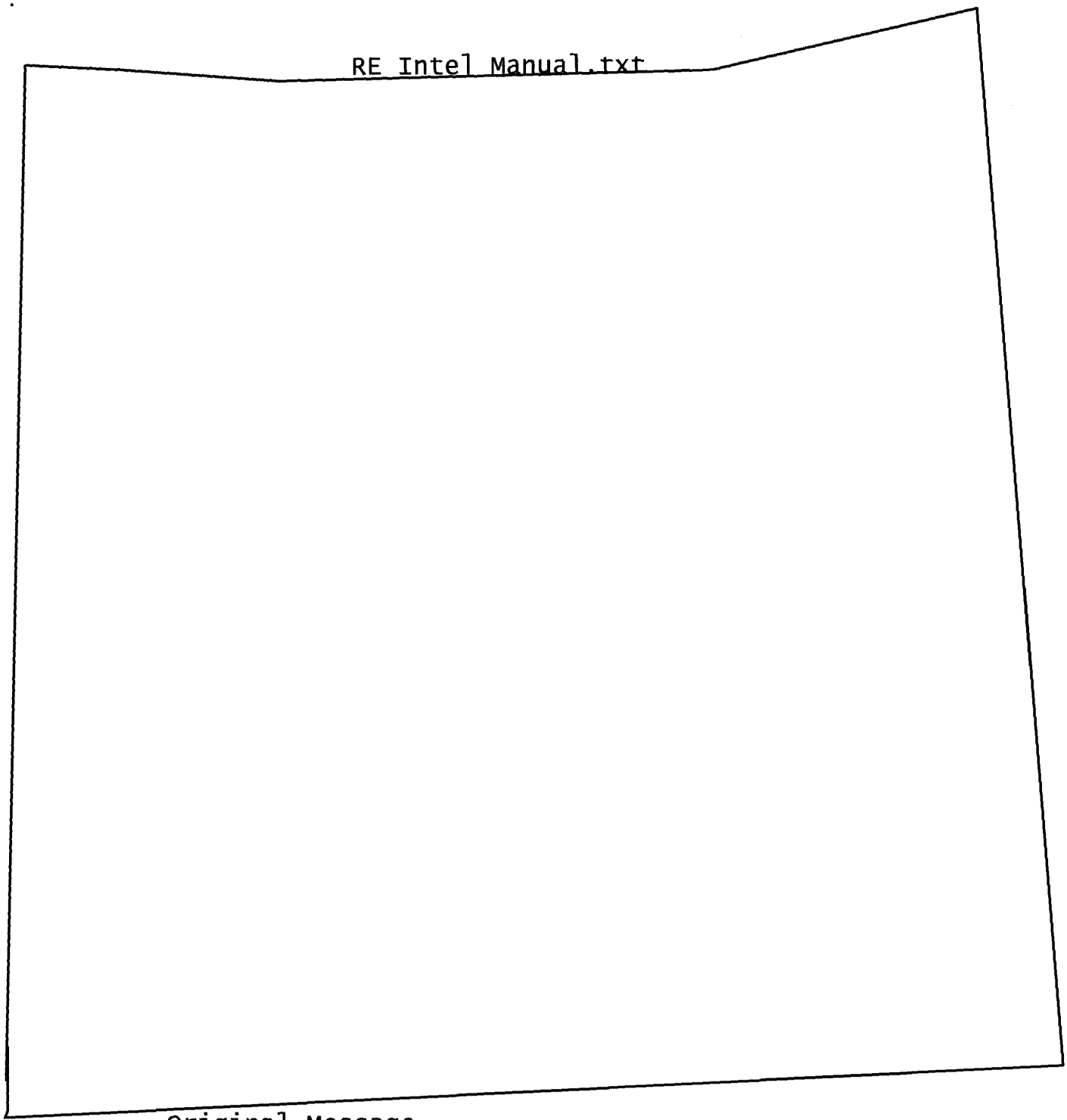
b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b5
b6
b7C

RE Intel Manual.txt



-----Original Message-----
From: (OGC) (FBI)
Sent: Monday, August 16, 2004 5:55 PM
To: (OGC) (FBI)

b6
b7C

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b6
b7C

RE Intel Manual.txt
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); [redacted] (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Intel Manual

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

b6
b7C

b5

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

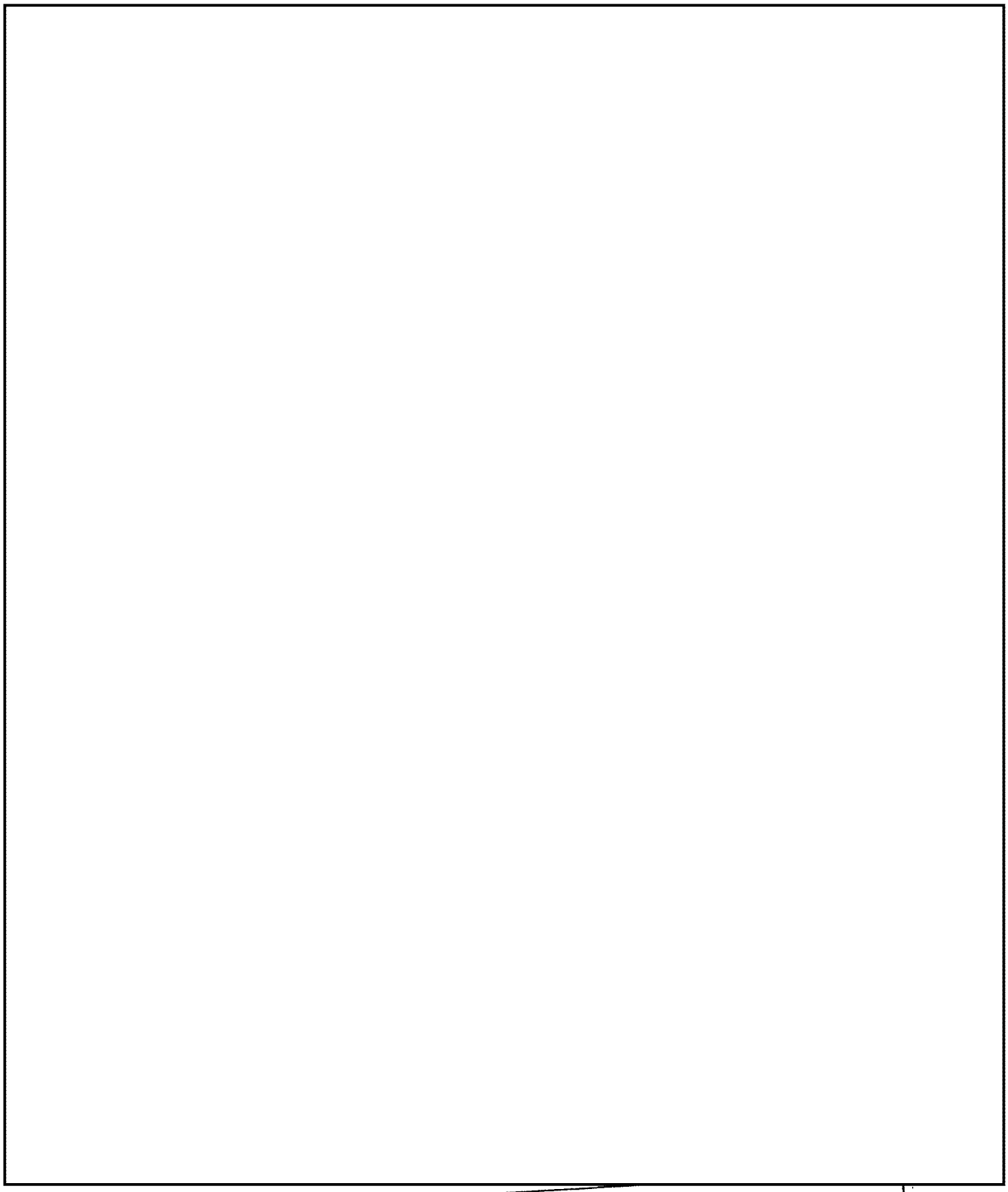
Comments from [redacted] 19 August, 5:55 pm

[redacted]

Comments from [redacted] 11 August, 7:40 pm b6 b5
b7C

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



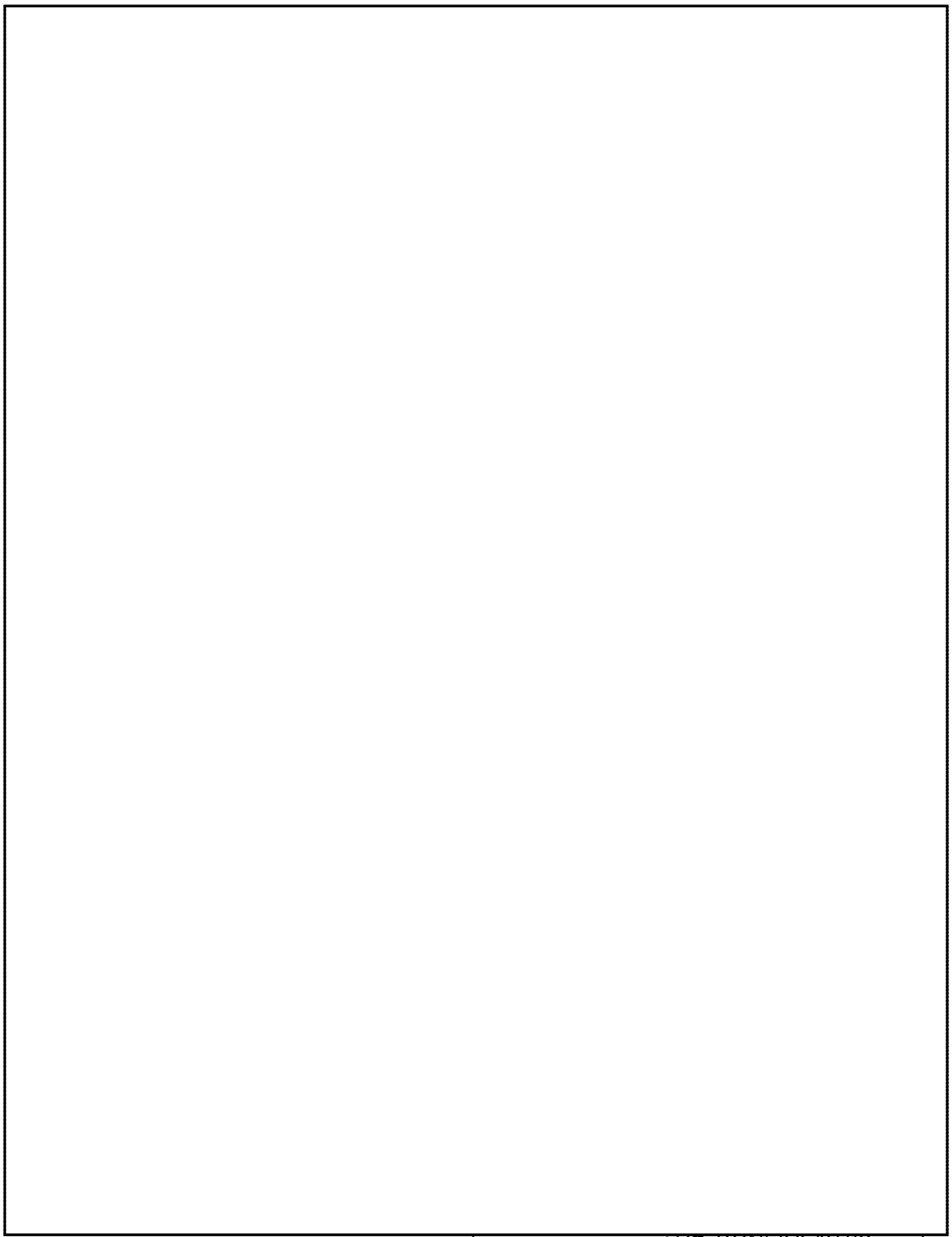
b5

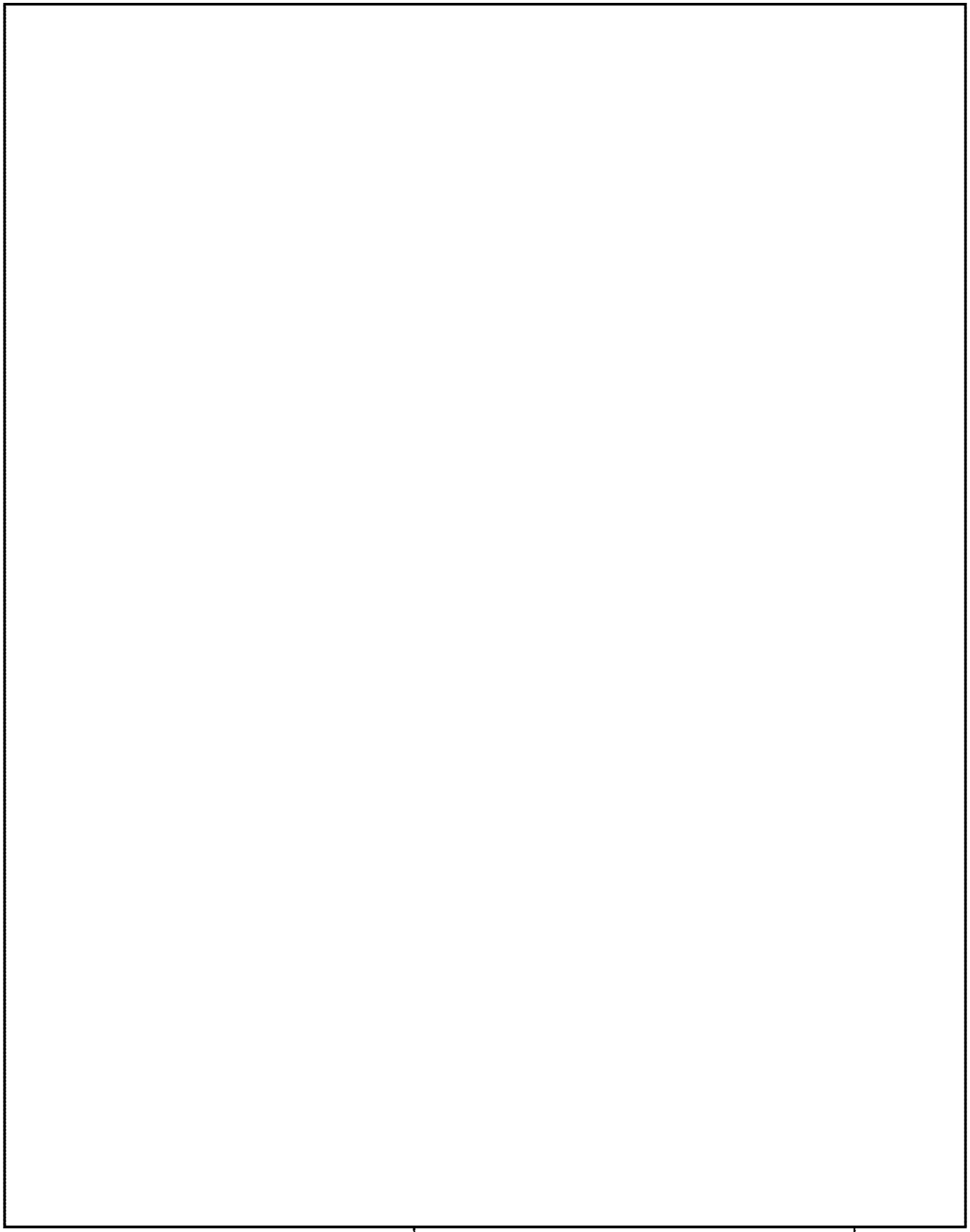
COMMENTS FROM [redacted] NSLB/Policy & Training Unit:

b6
b7C

b5

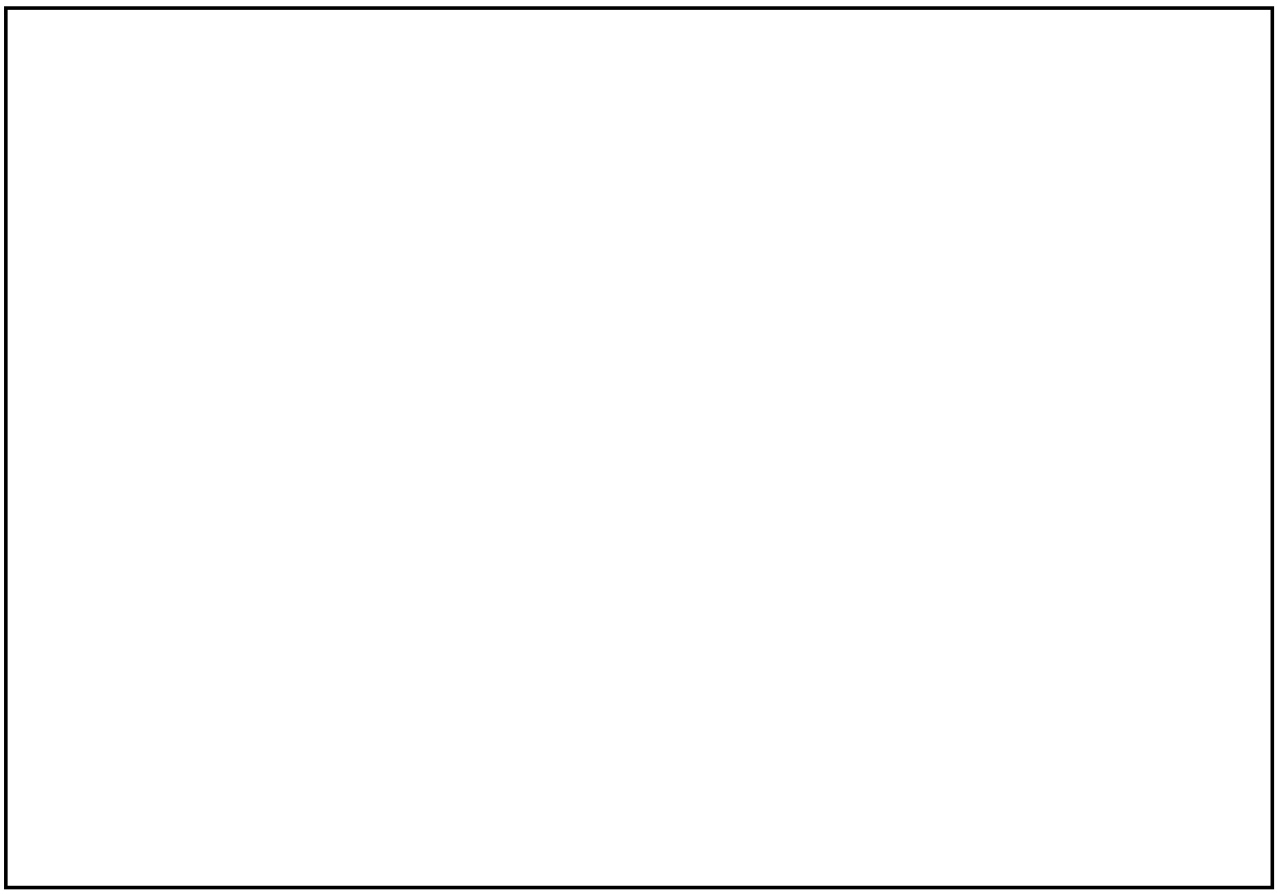
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT





PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

DRAFT: 9/23/04 Deleted: 7/29/04

[redacted] b5

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-06-2005 BY 65179 DMH/JHF 05-CV-0845

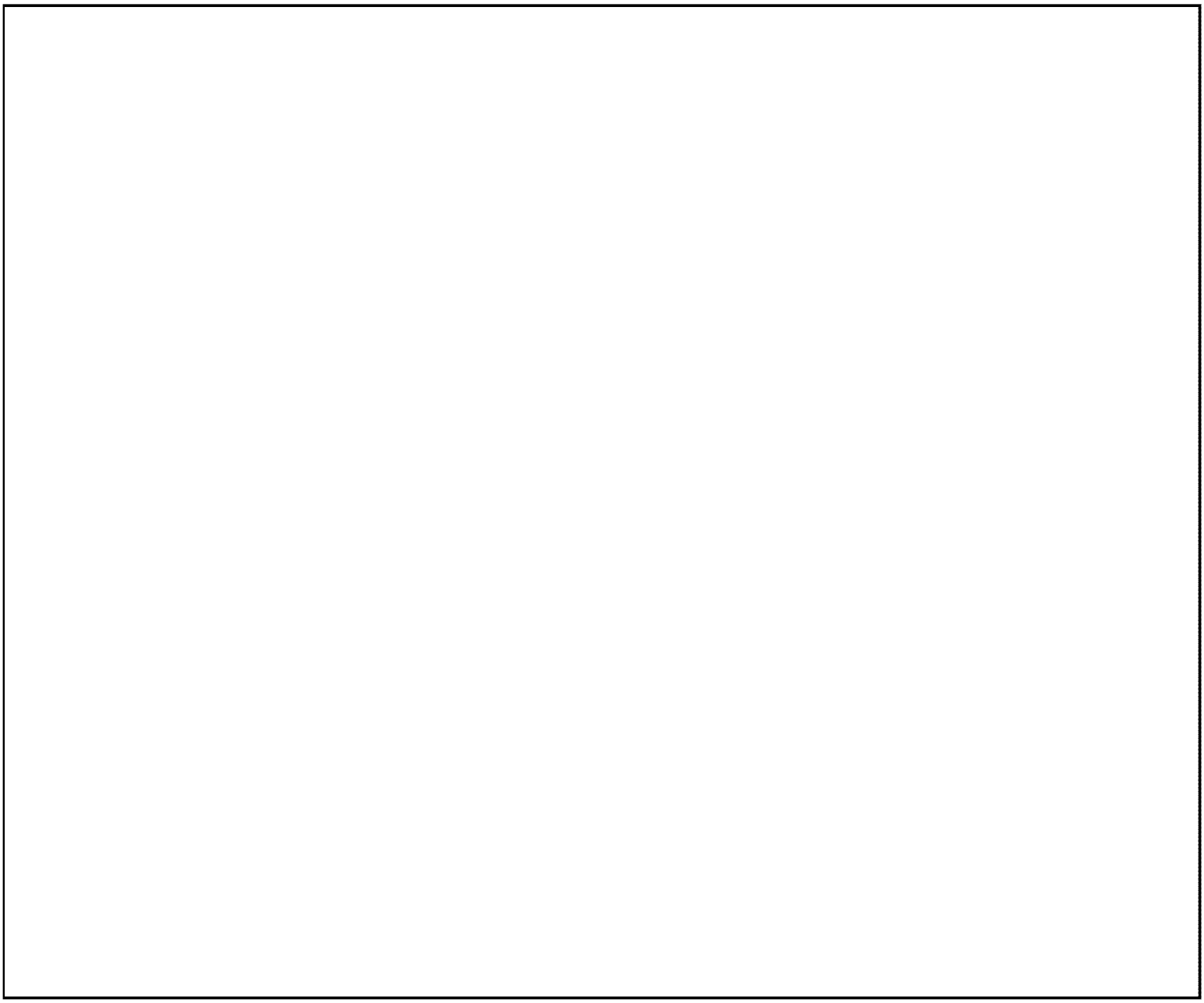
[redacted] b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

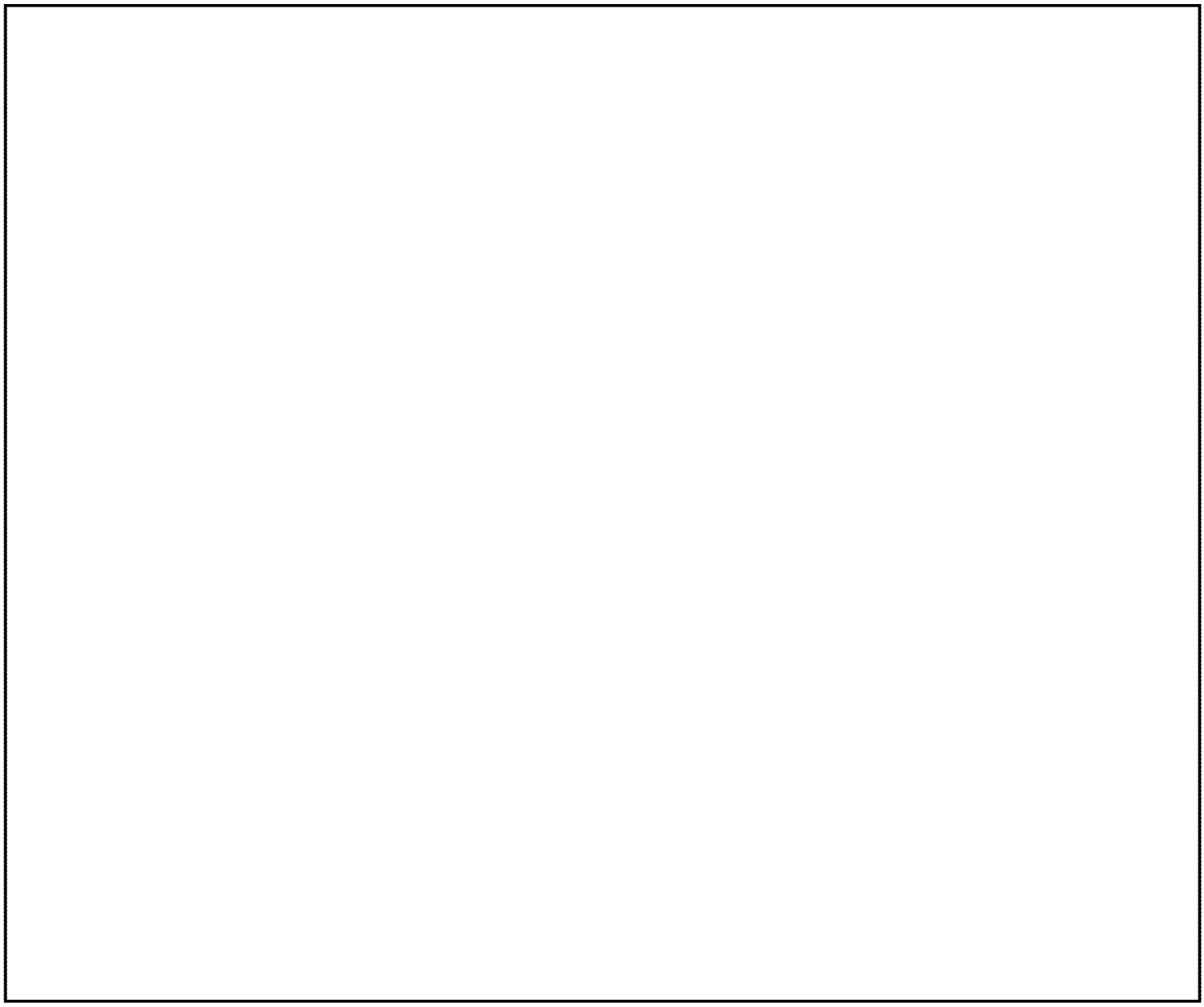
Introduction:

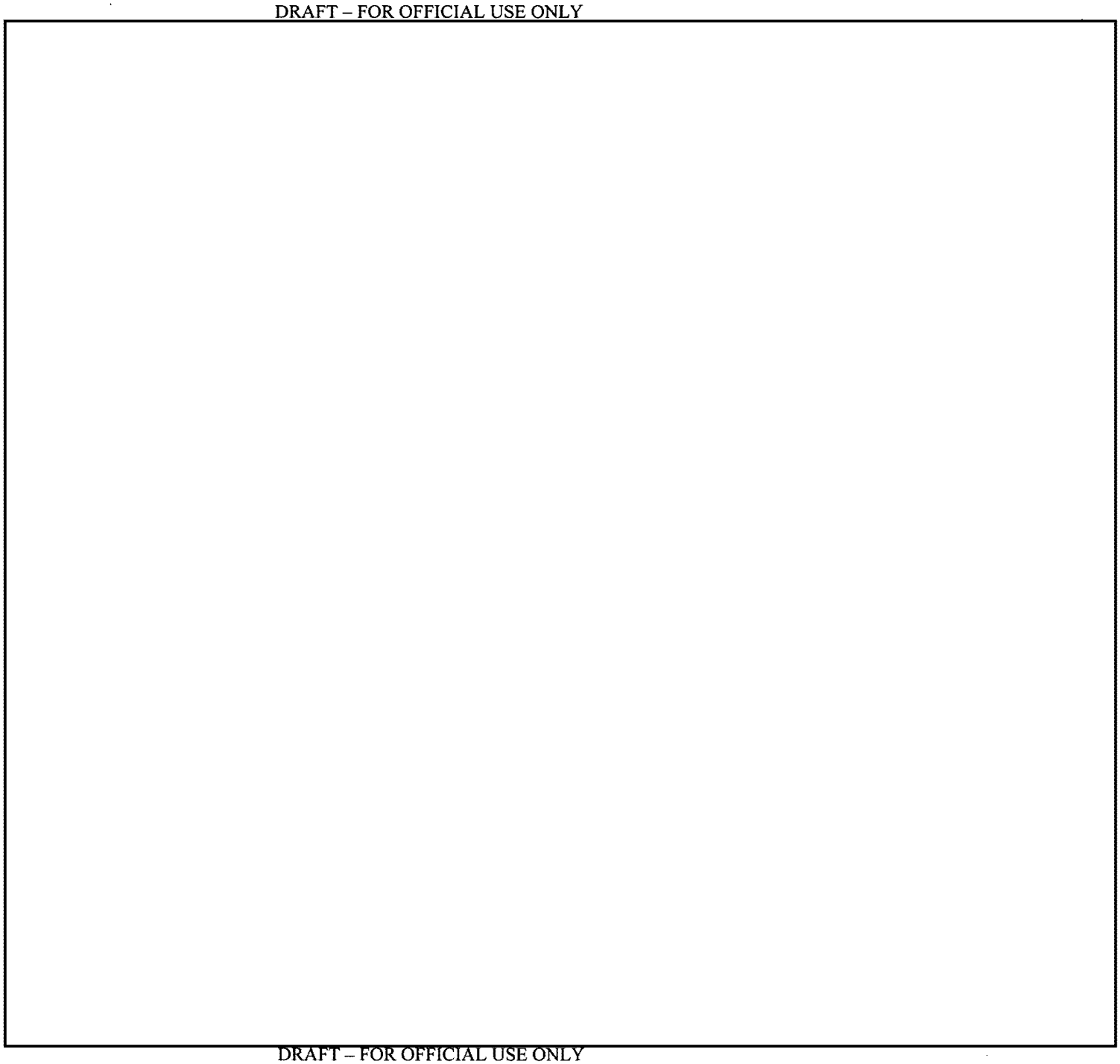
[redacted] b5

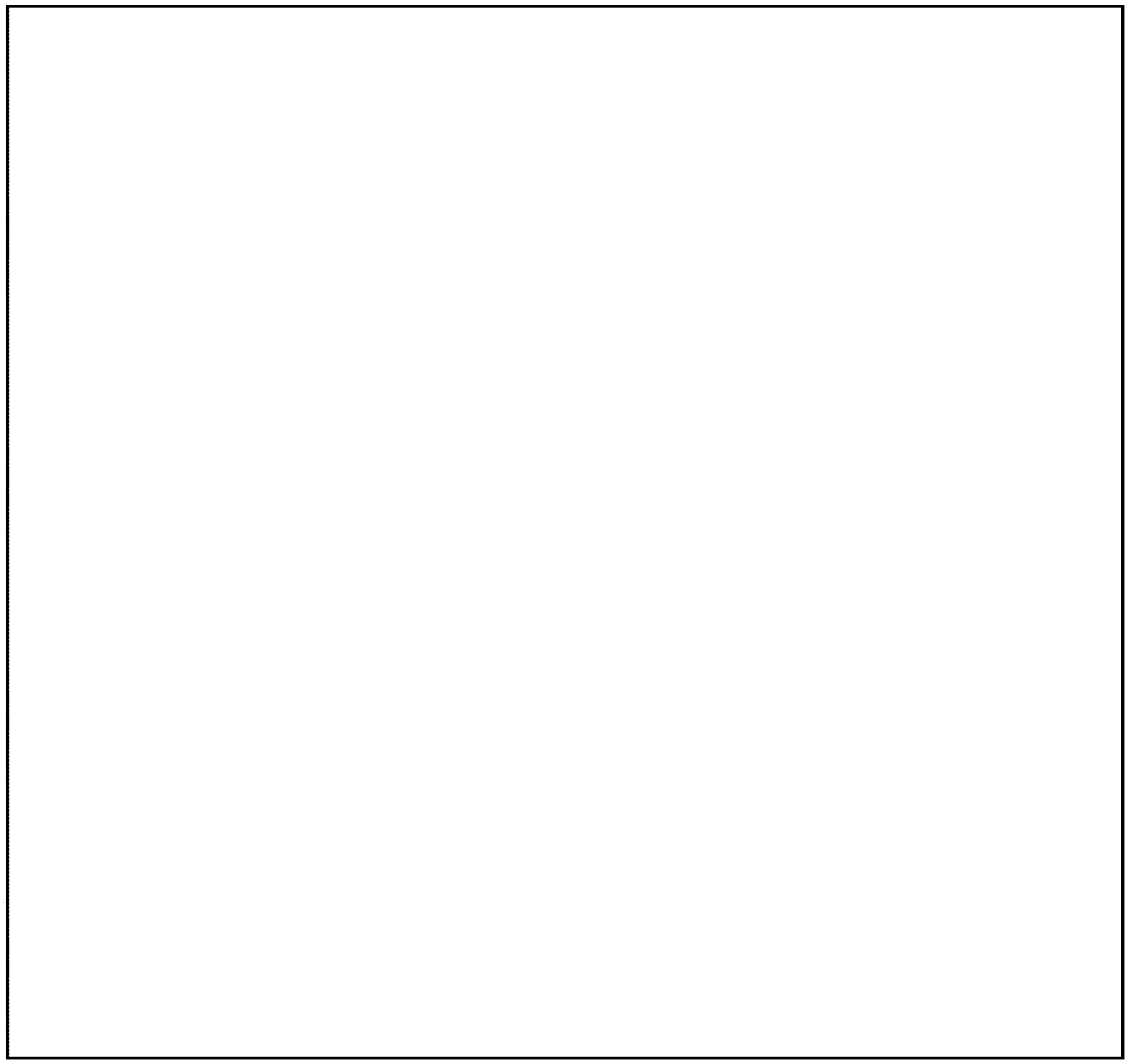
b5

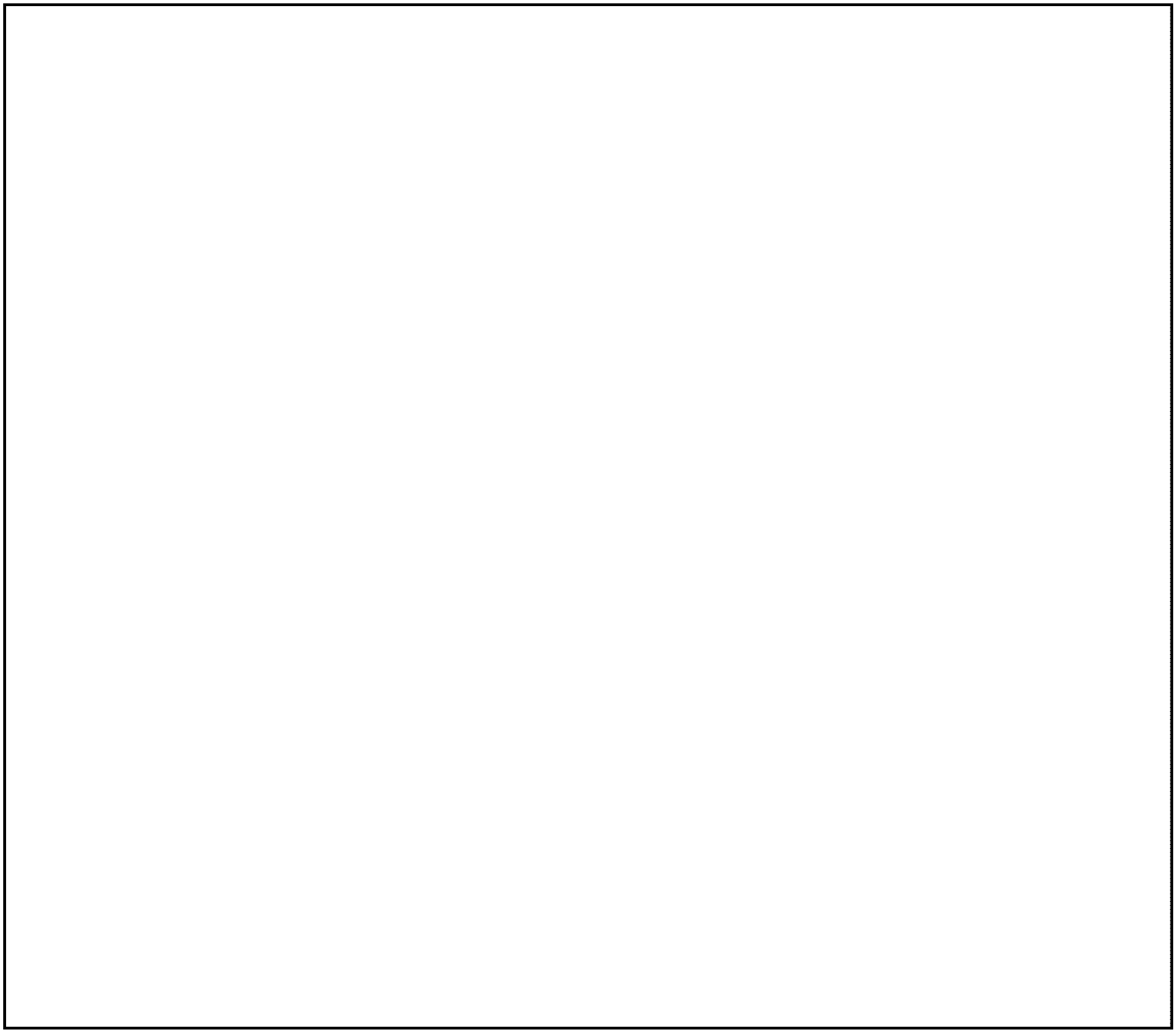


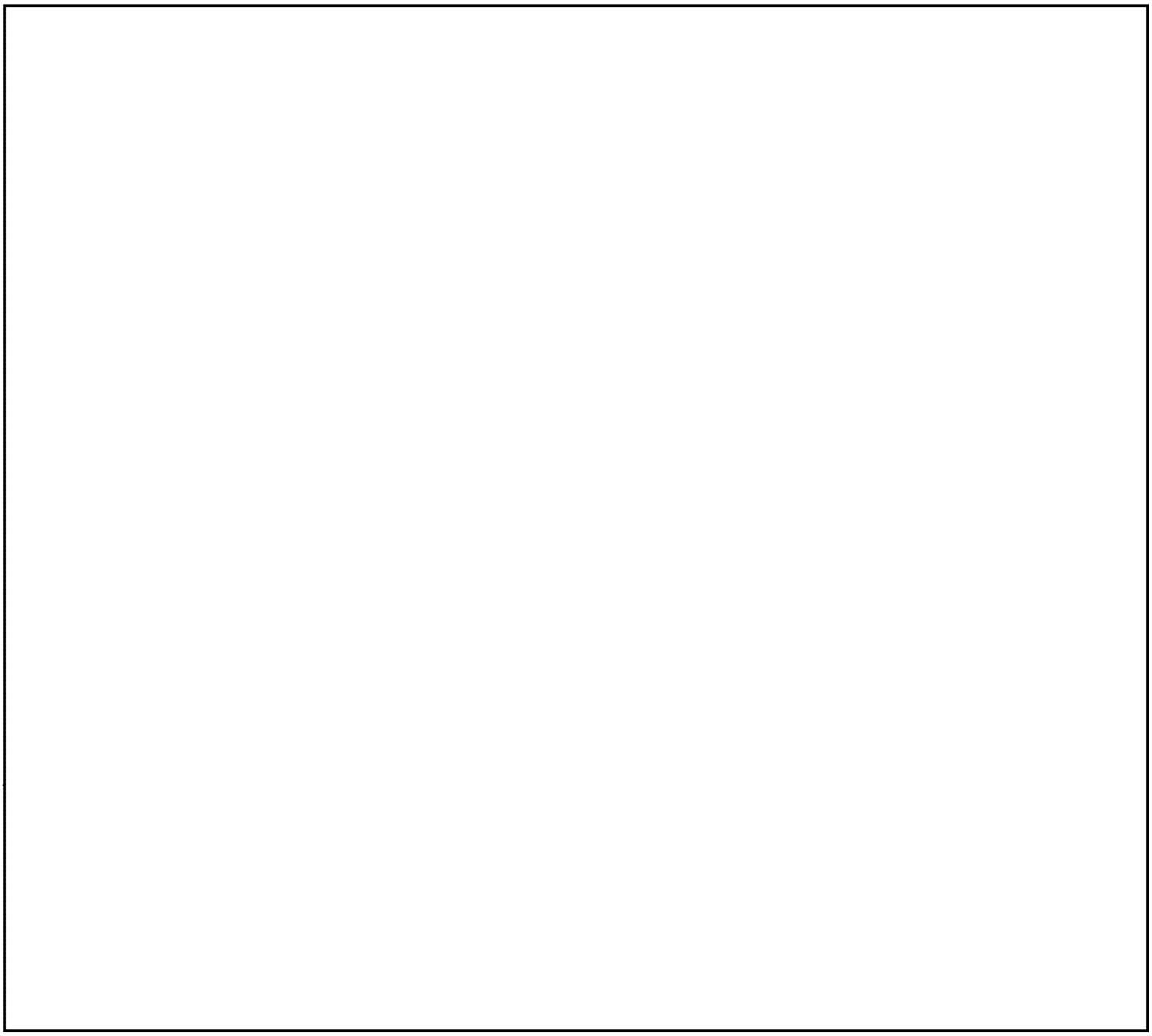
b5



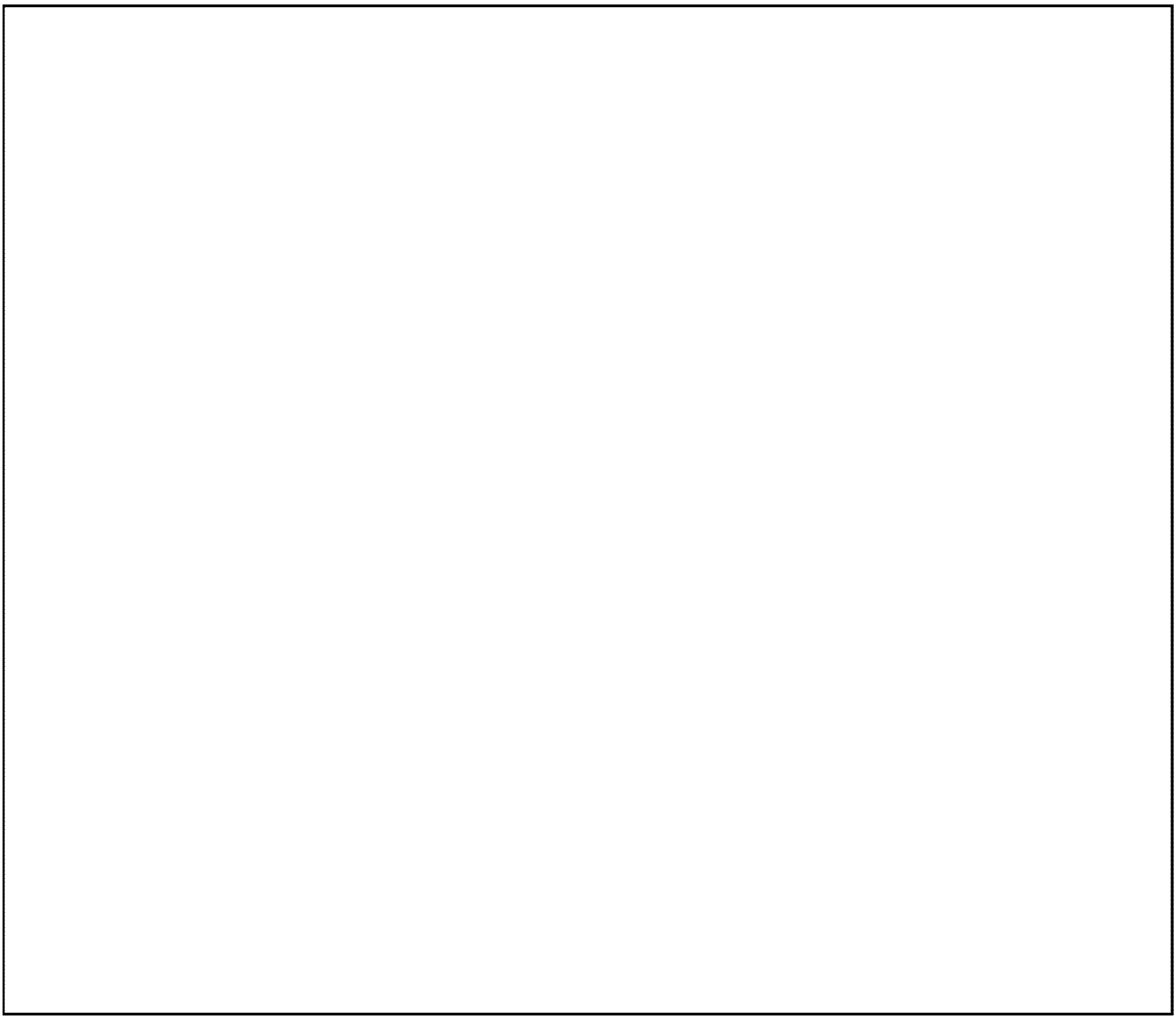


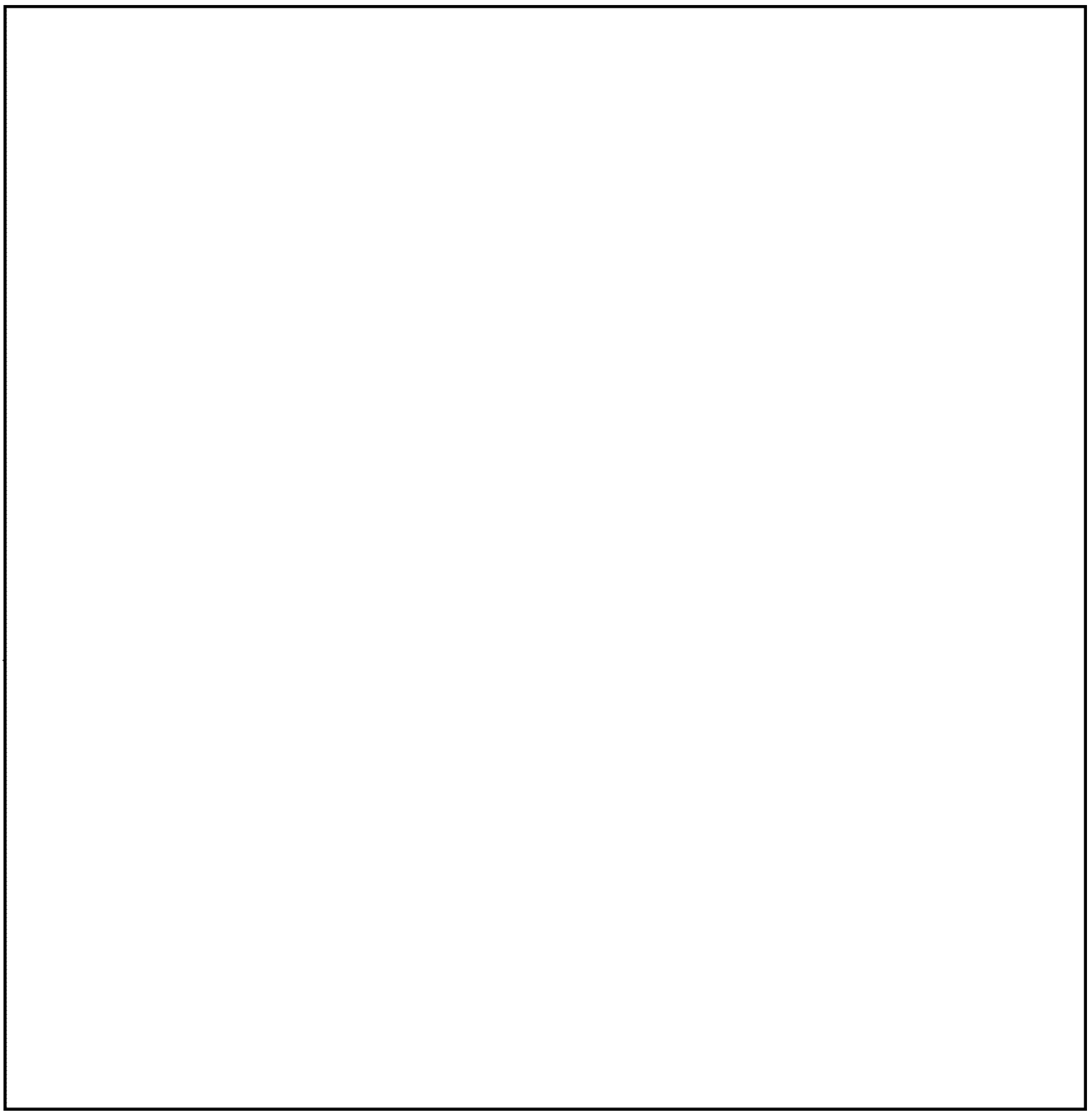




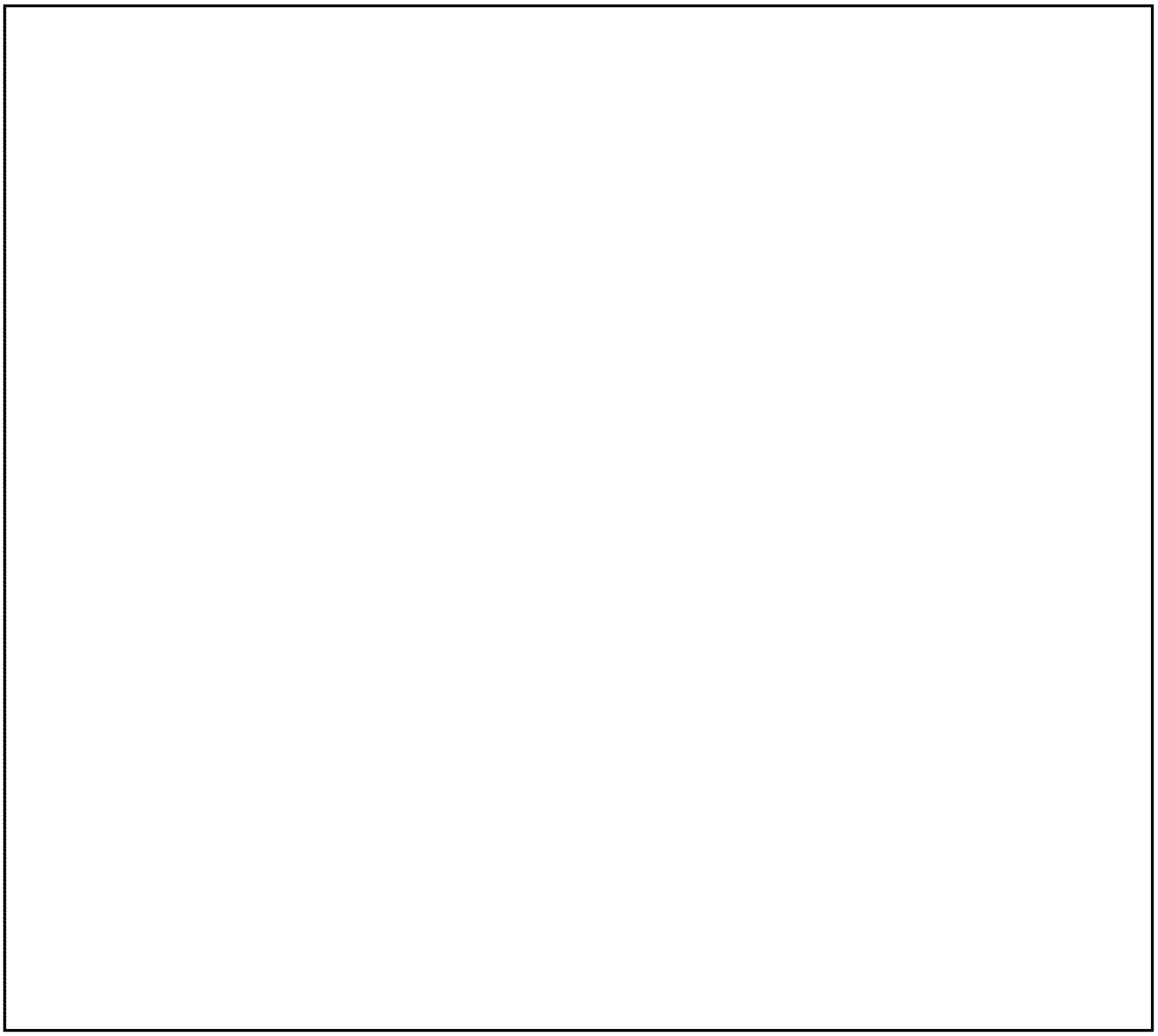


b5

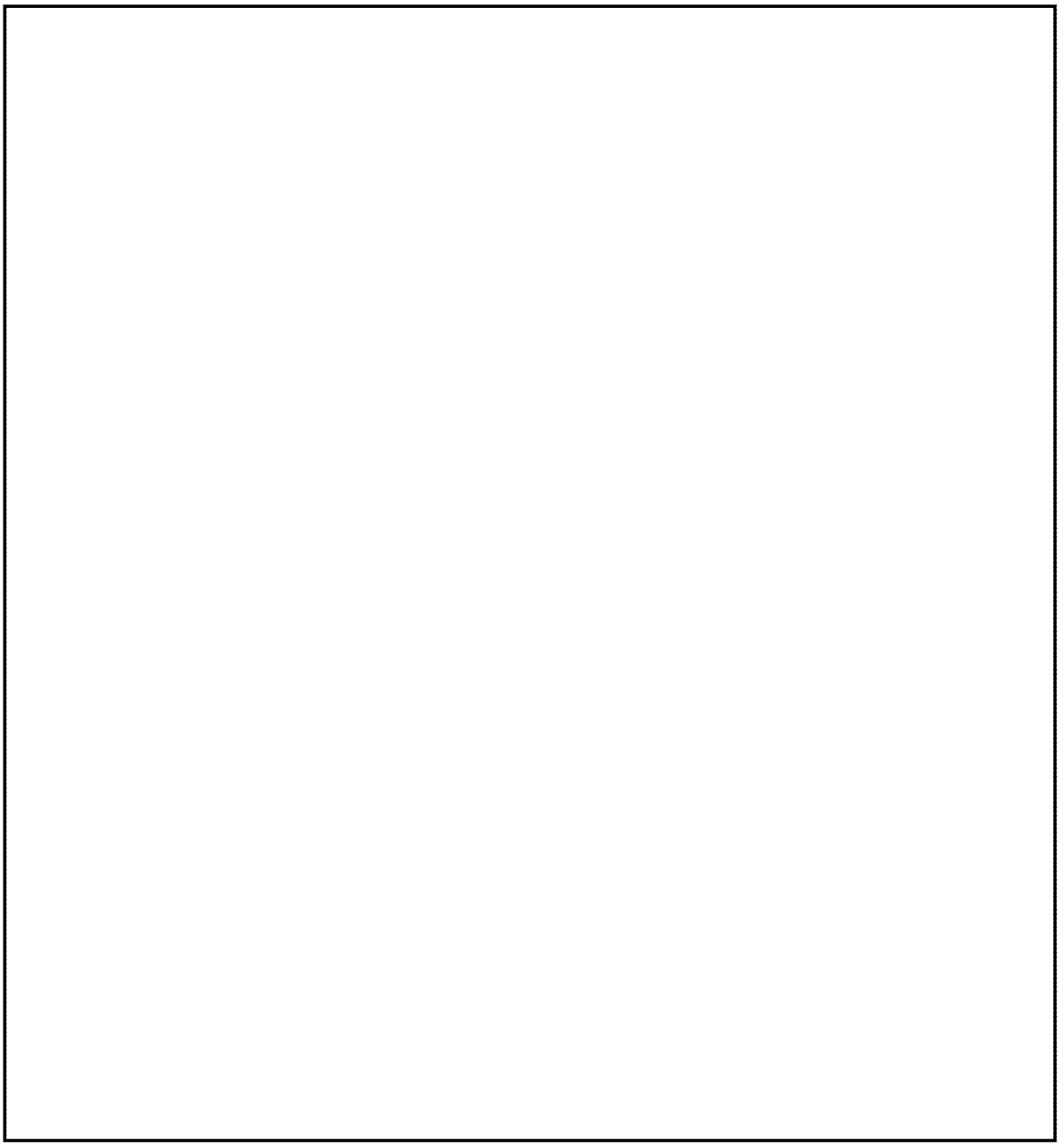




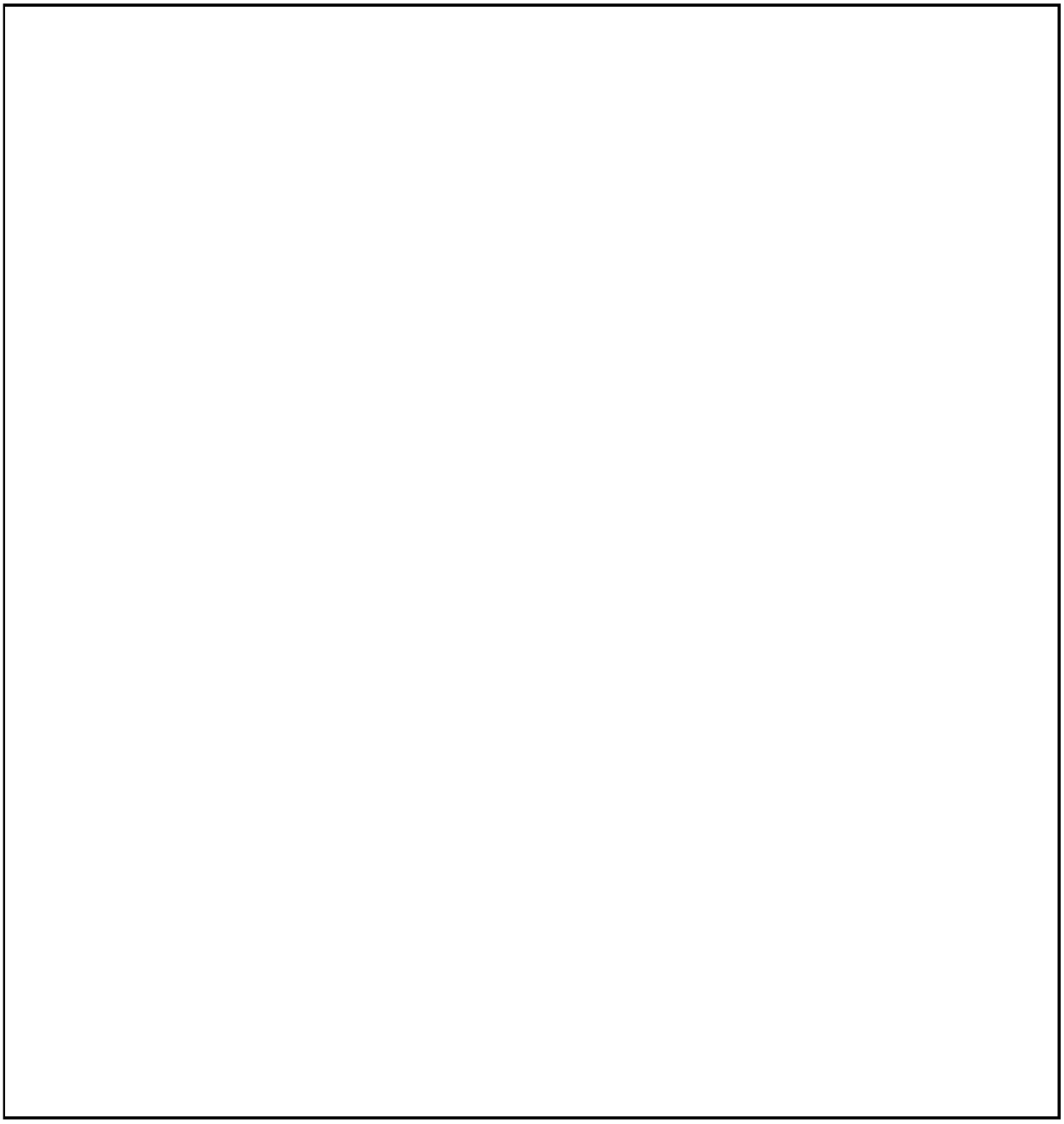
b5



b5



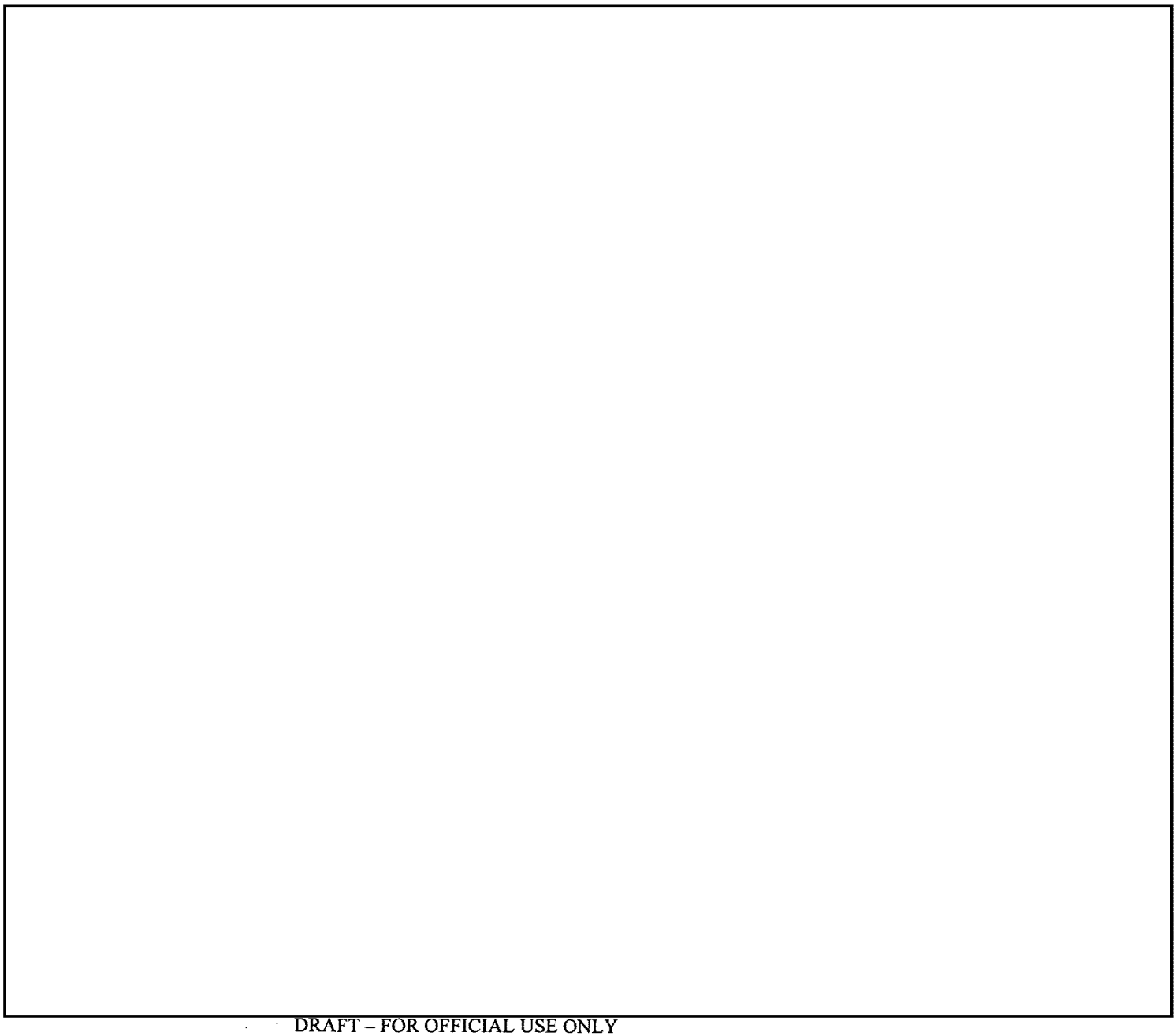
b5

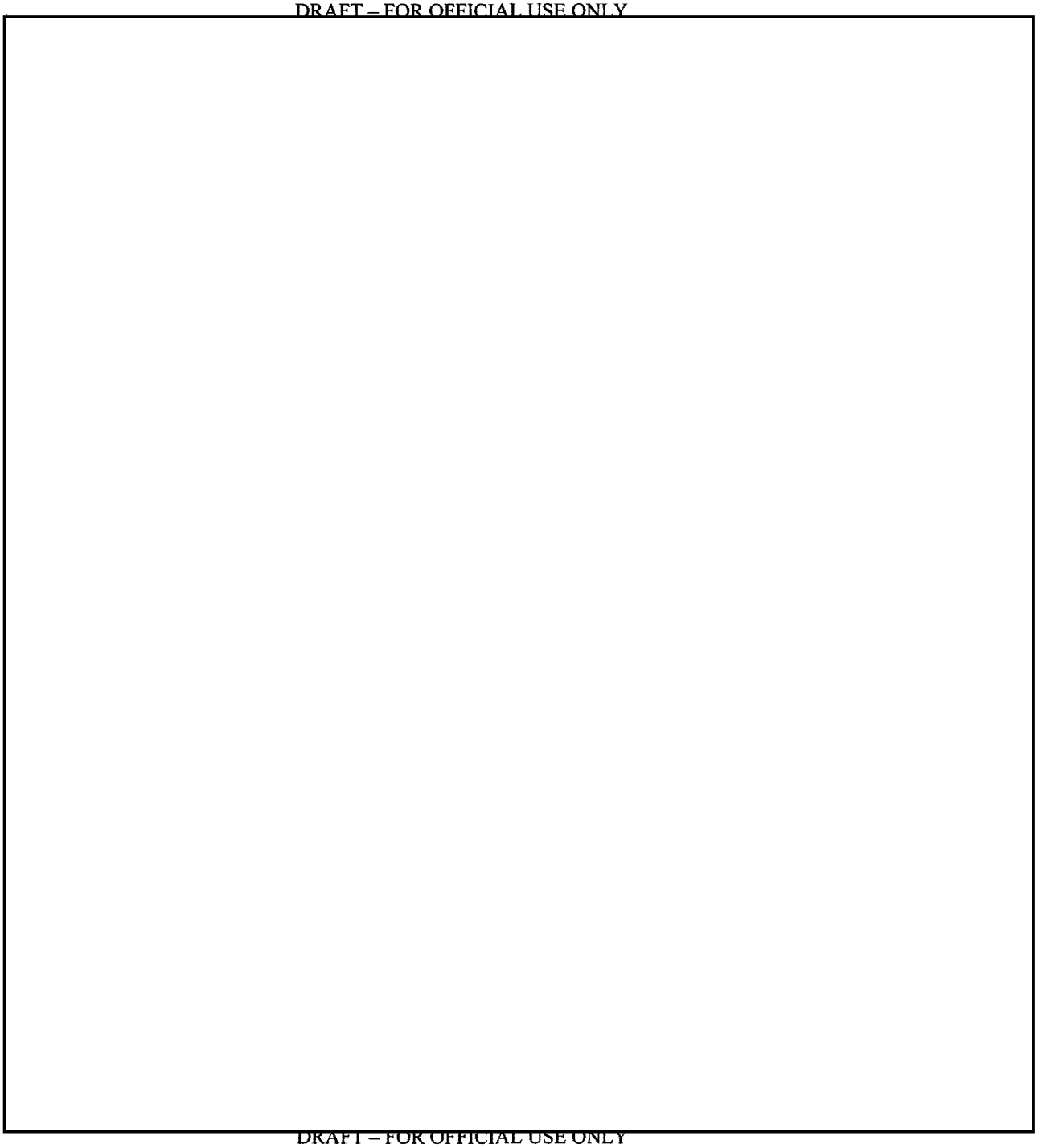


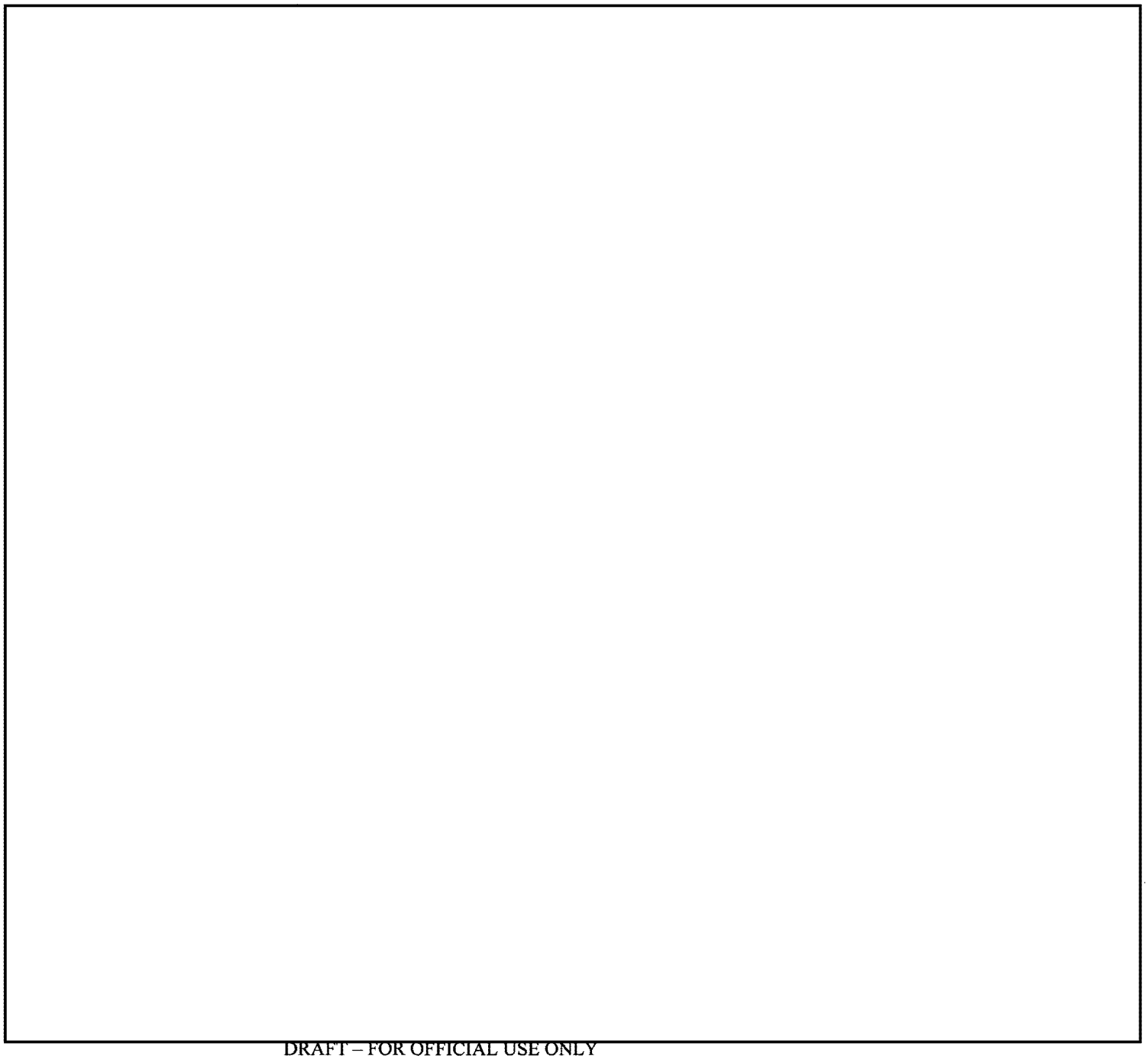
b5

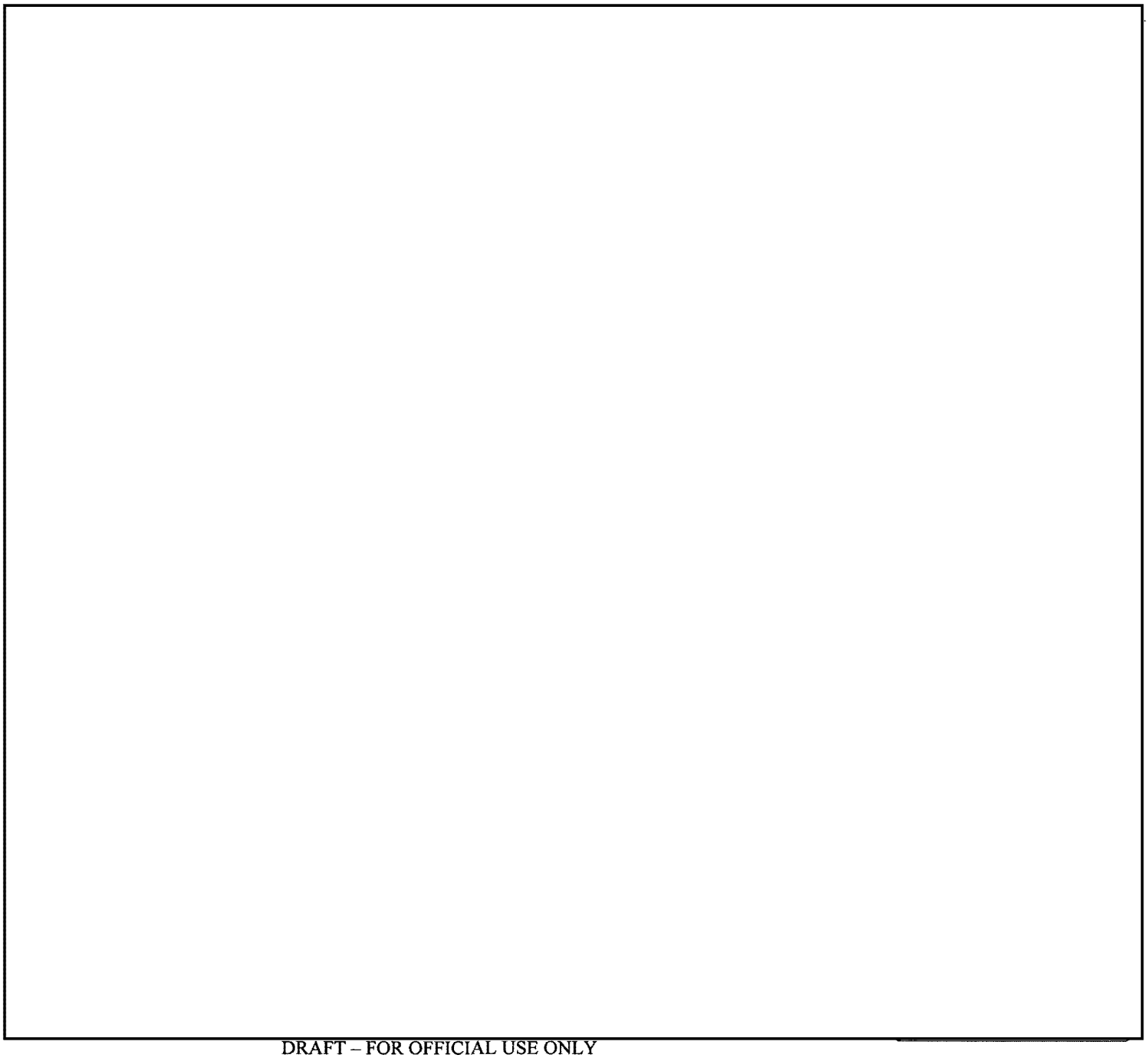
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

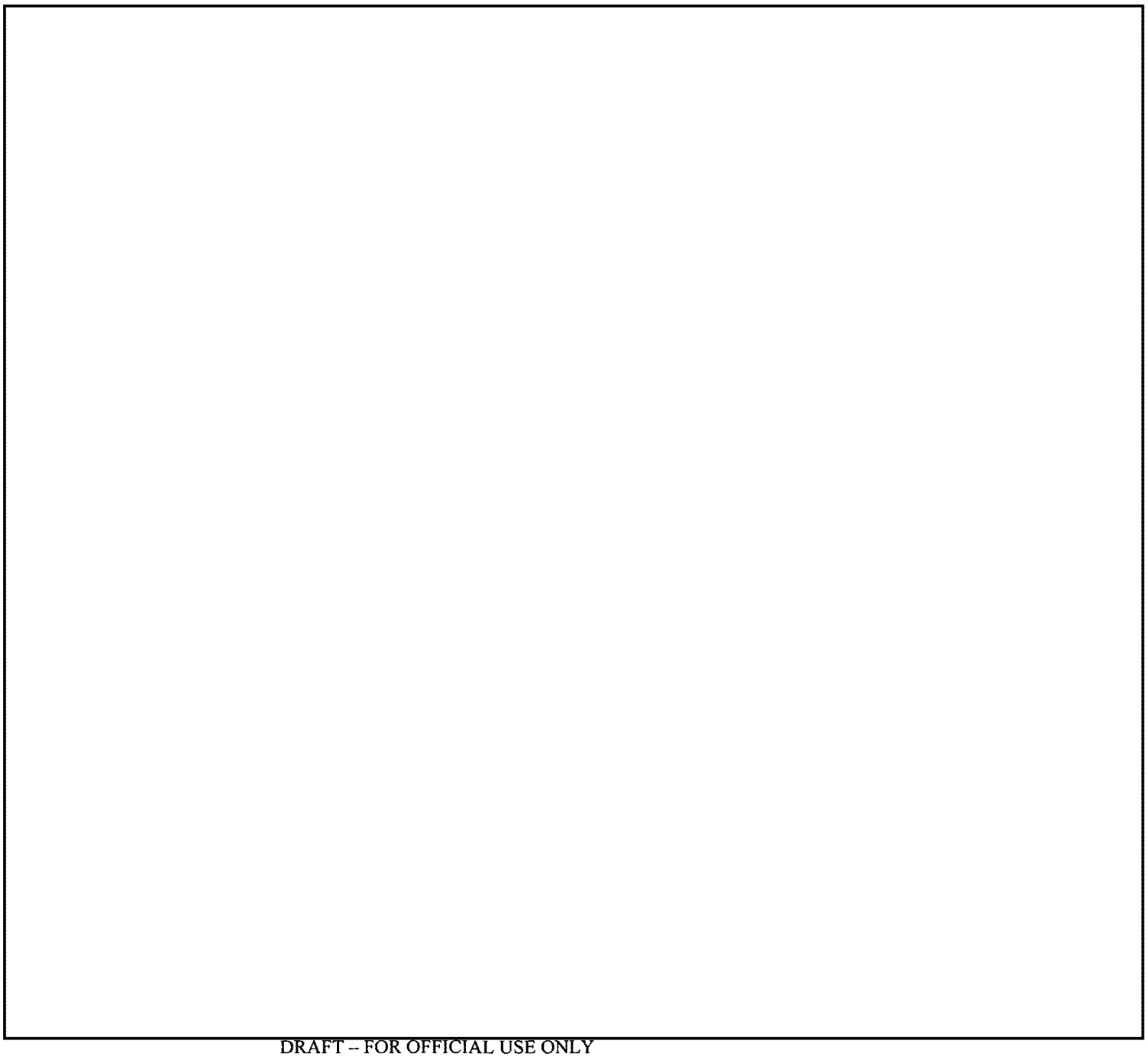






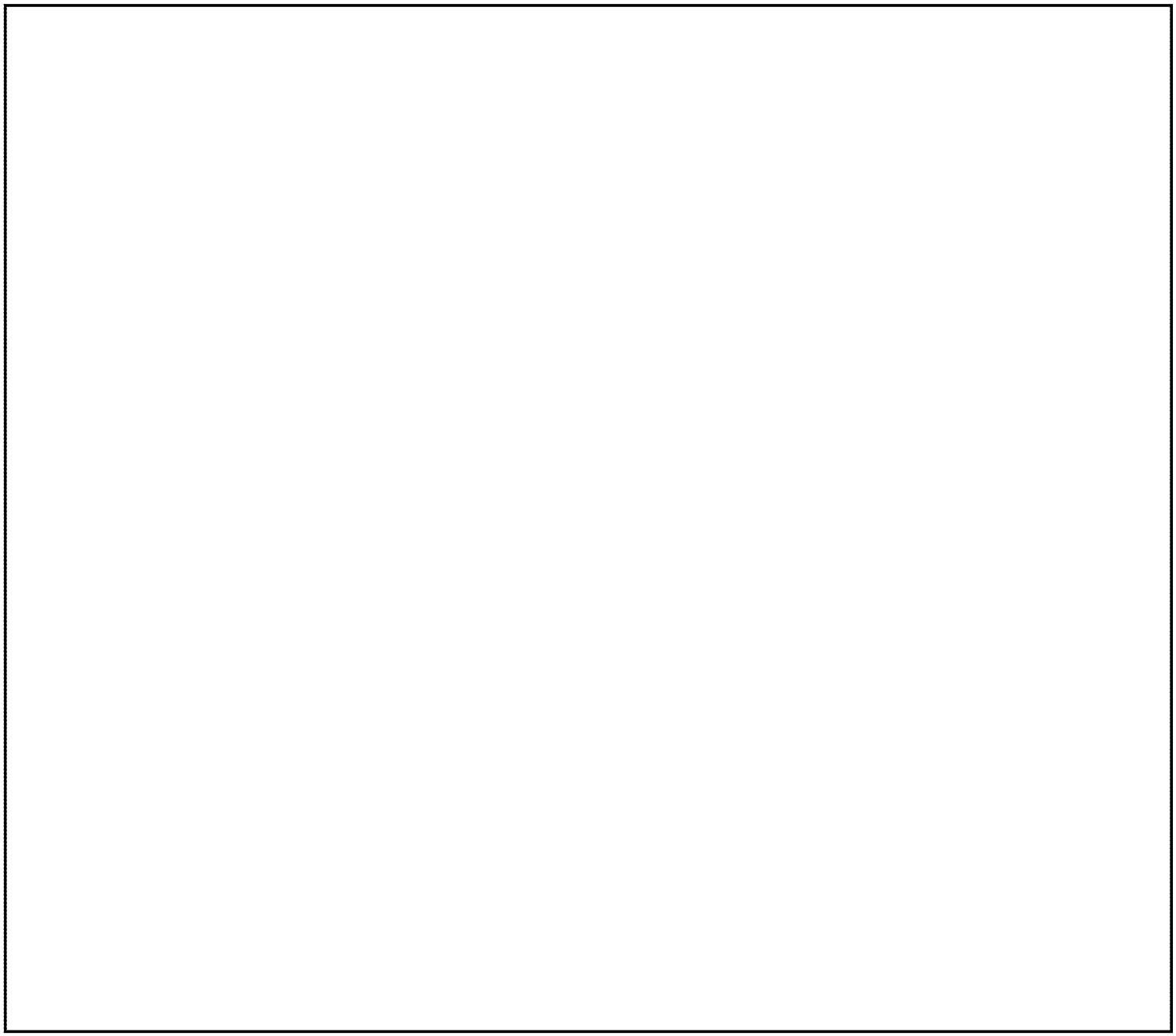


b5



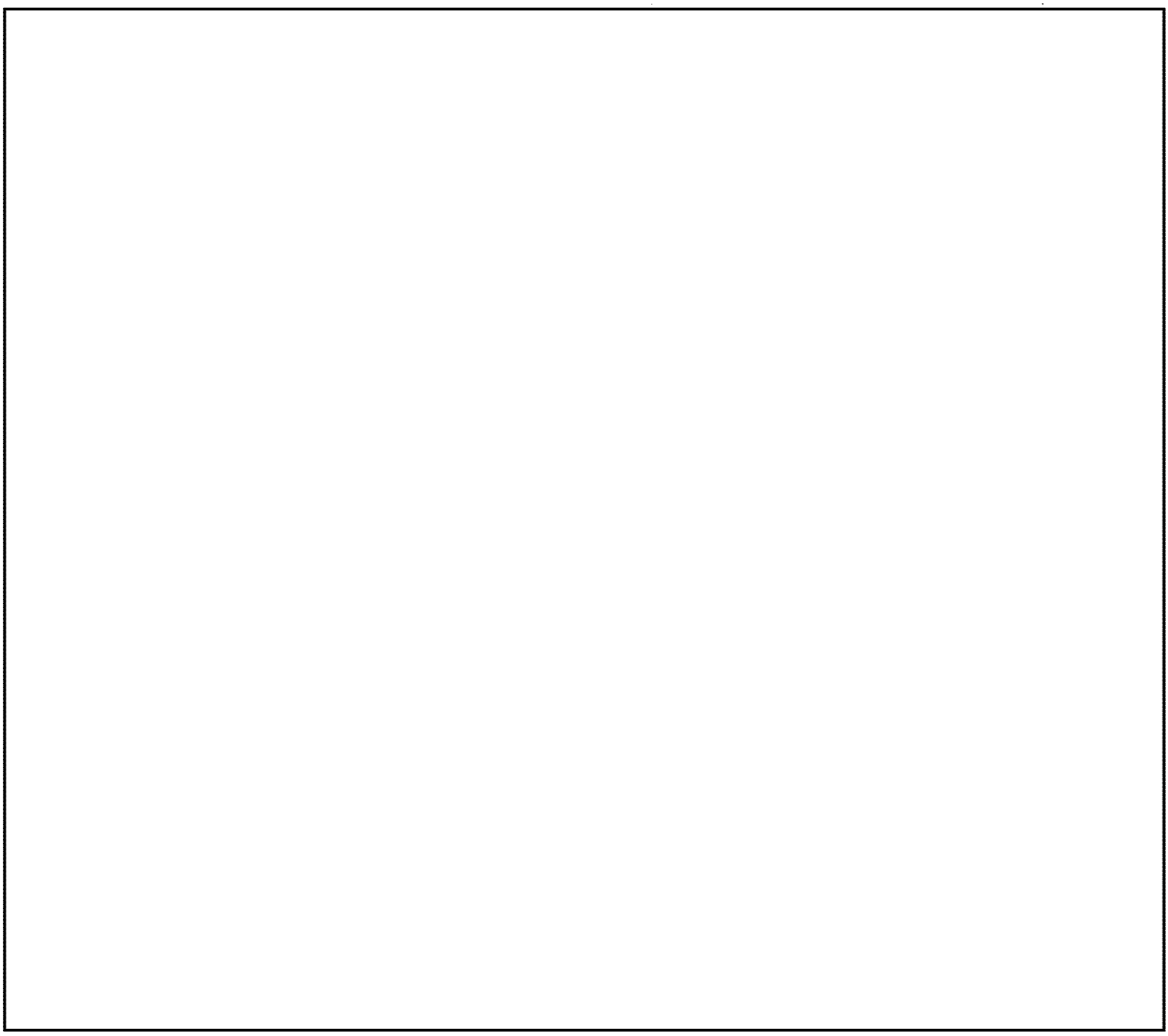
b5

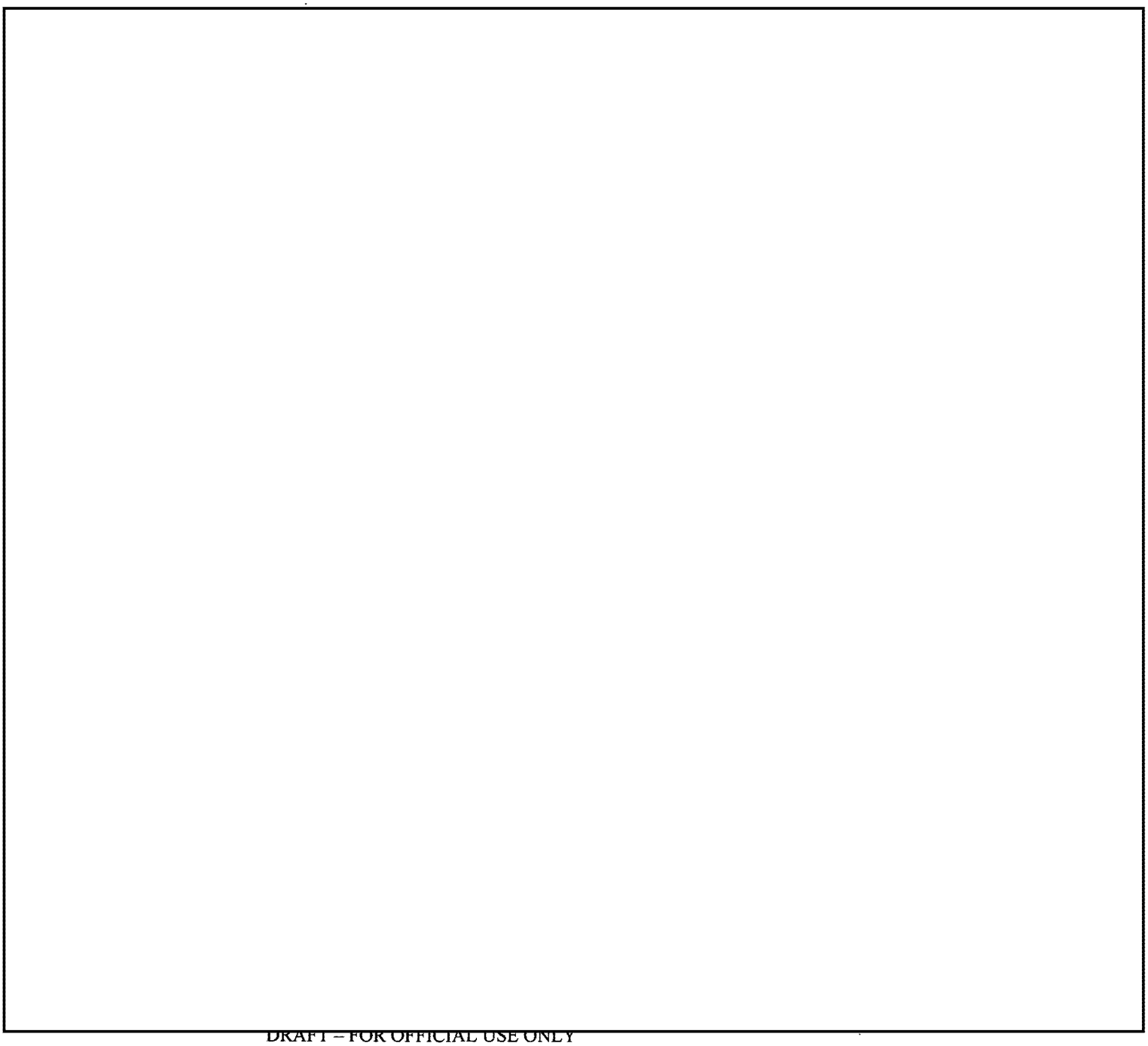
b5

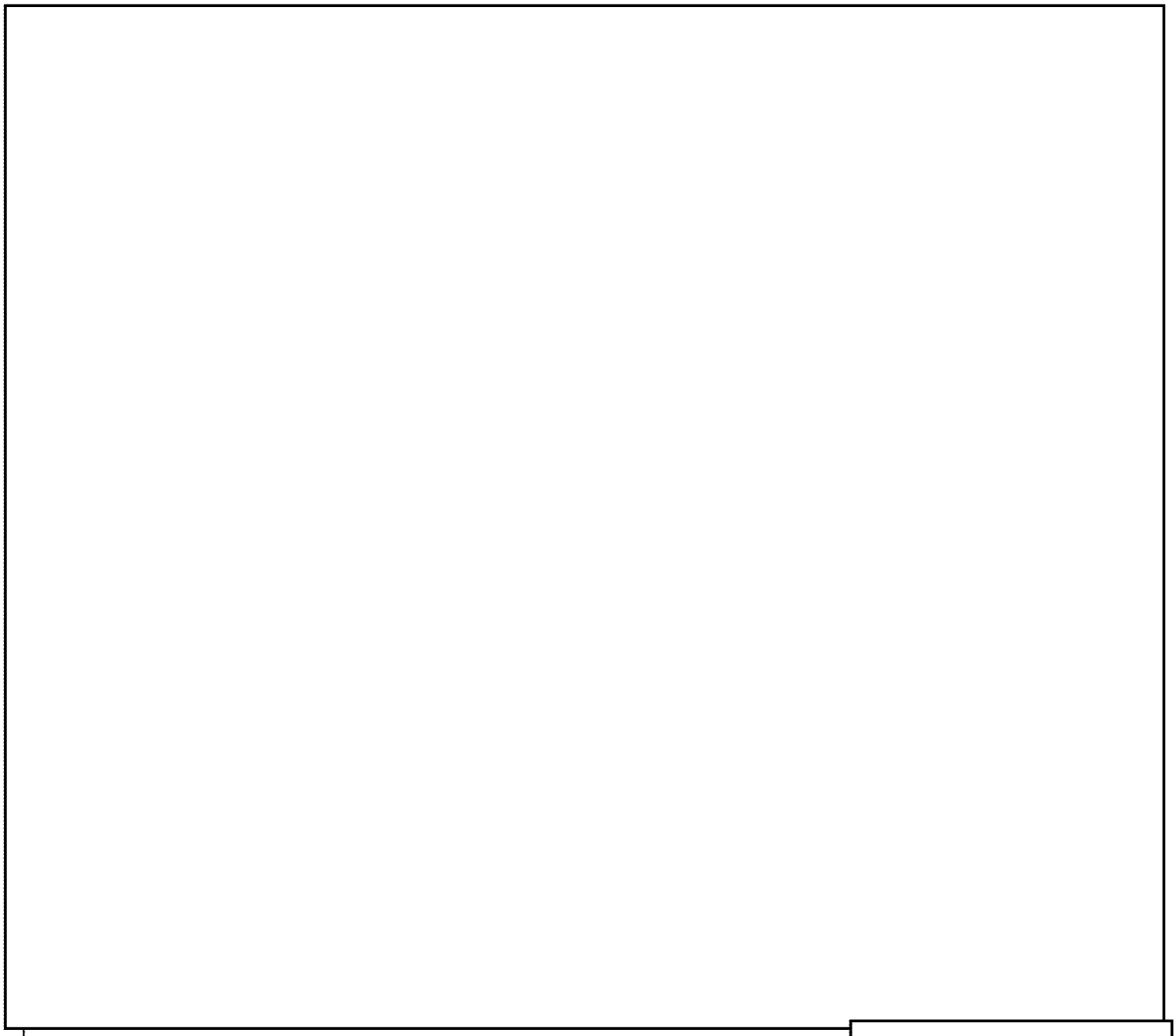


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

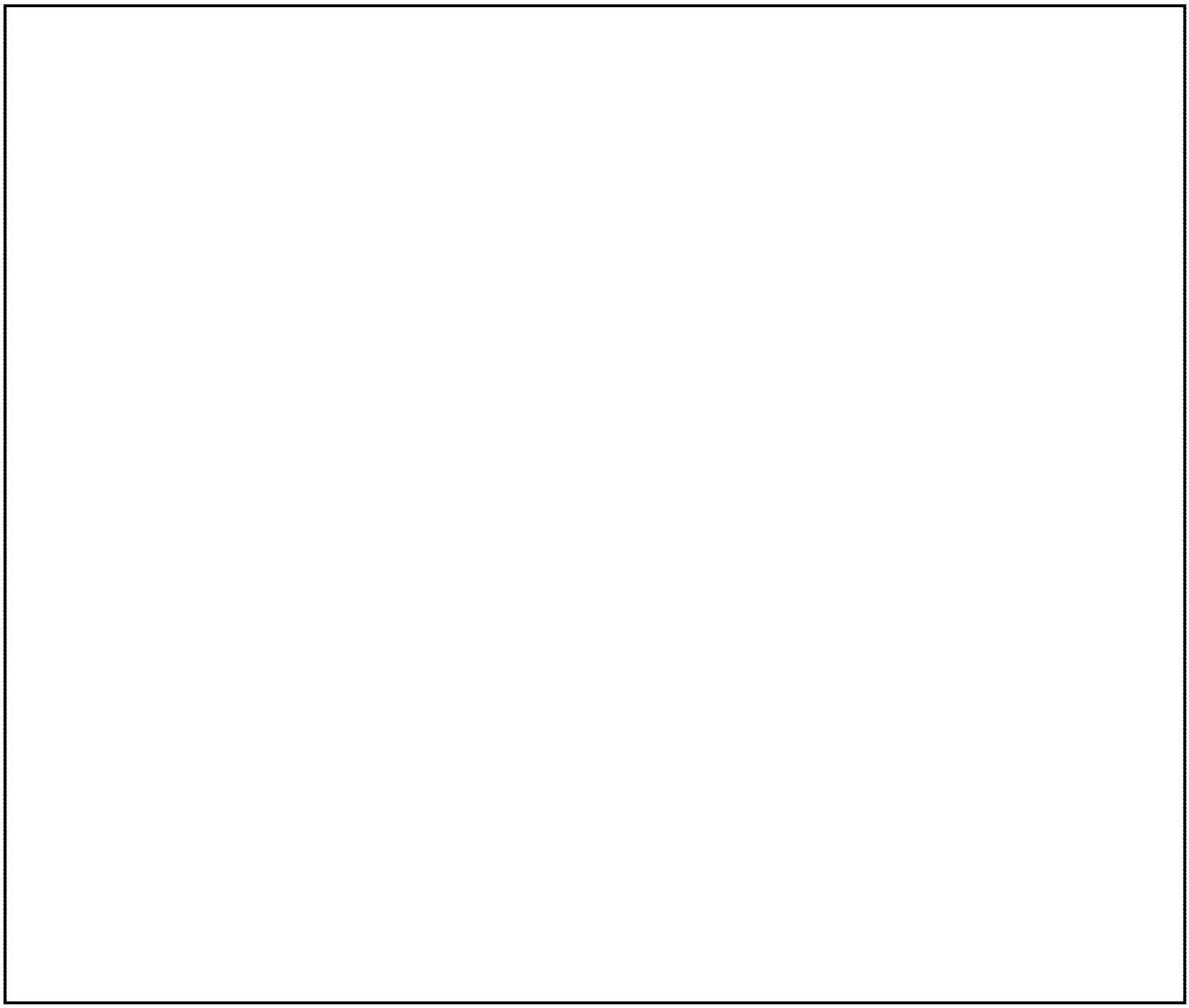
b5

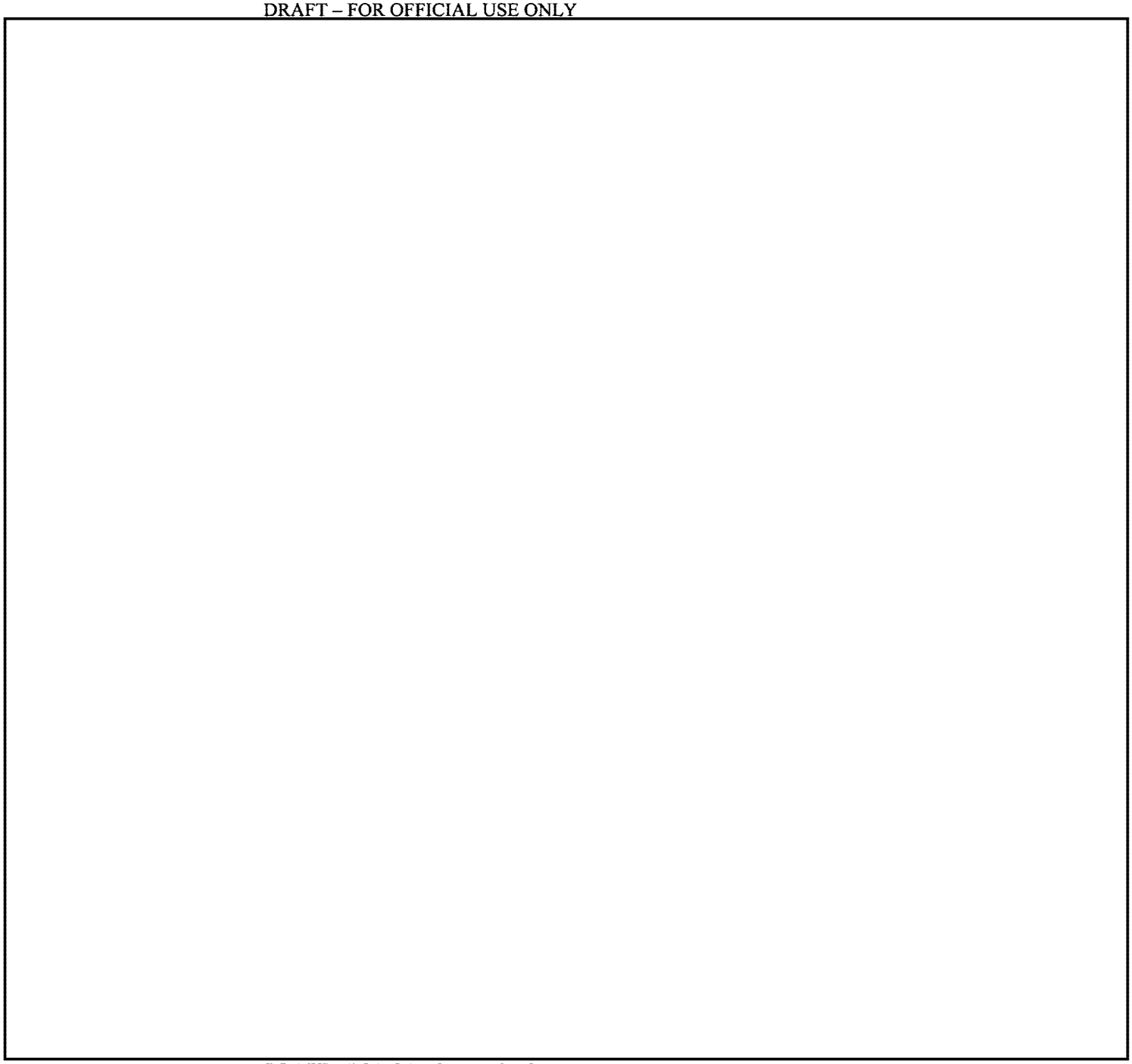






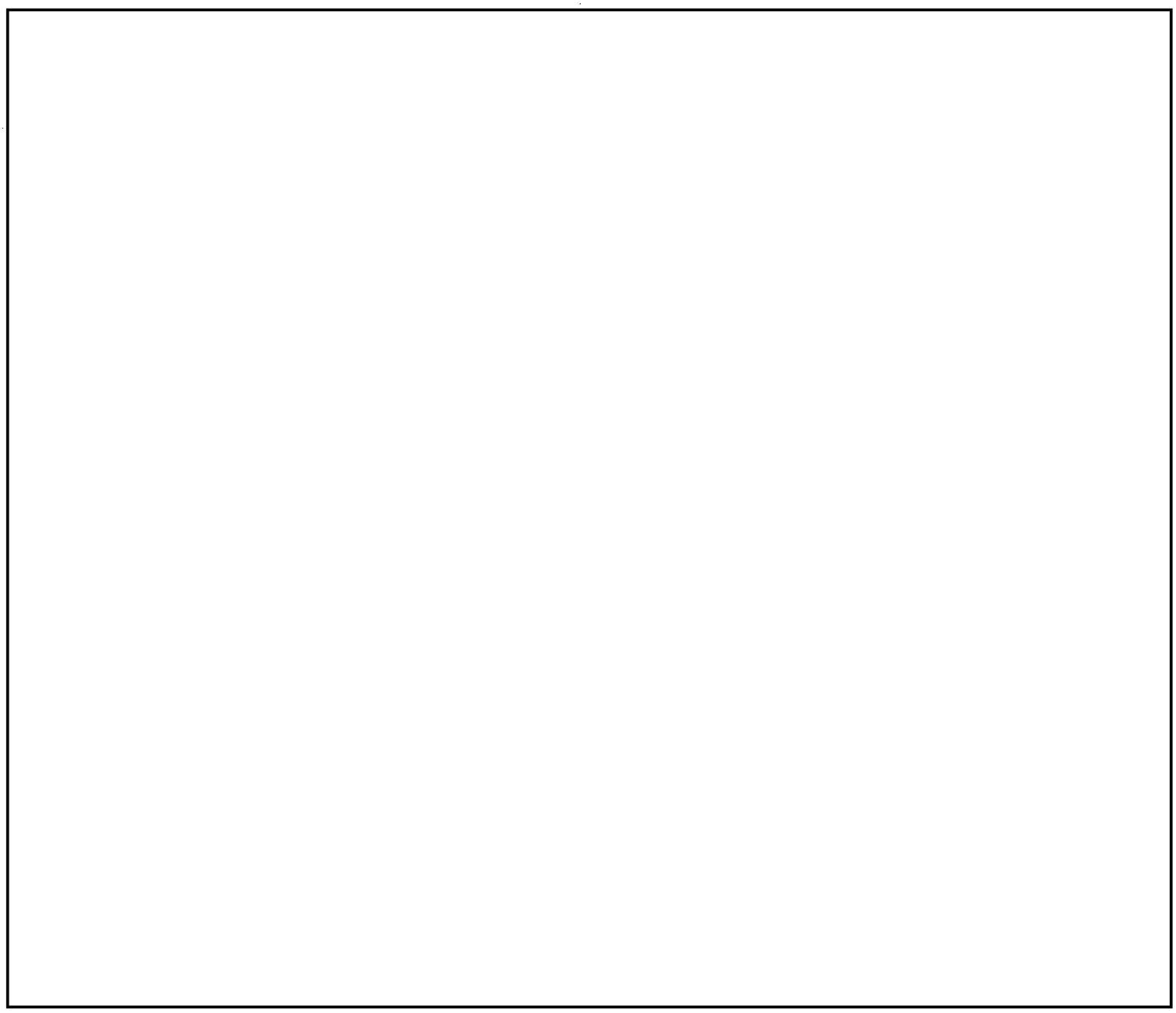
b5

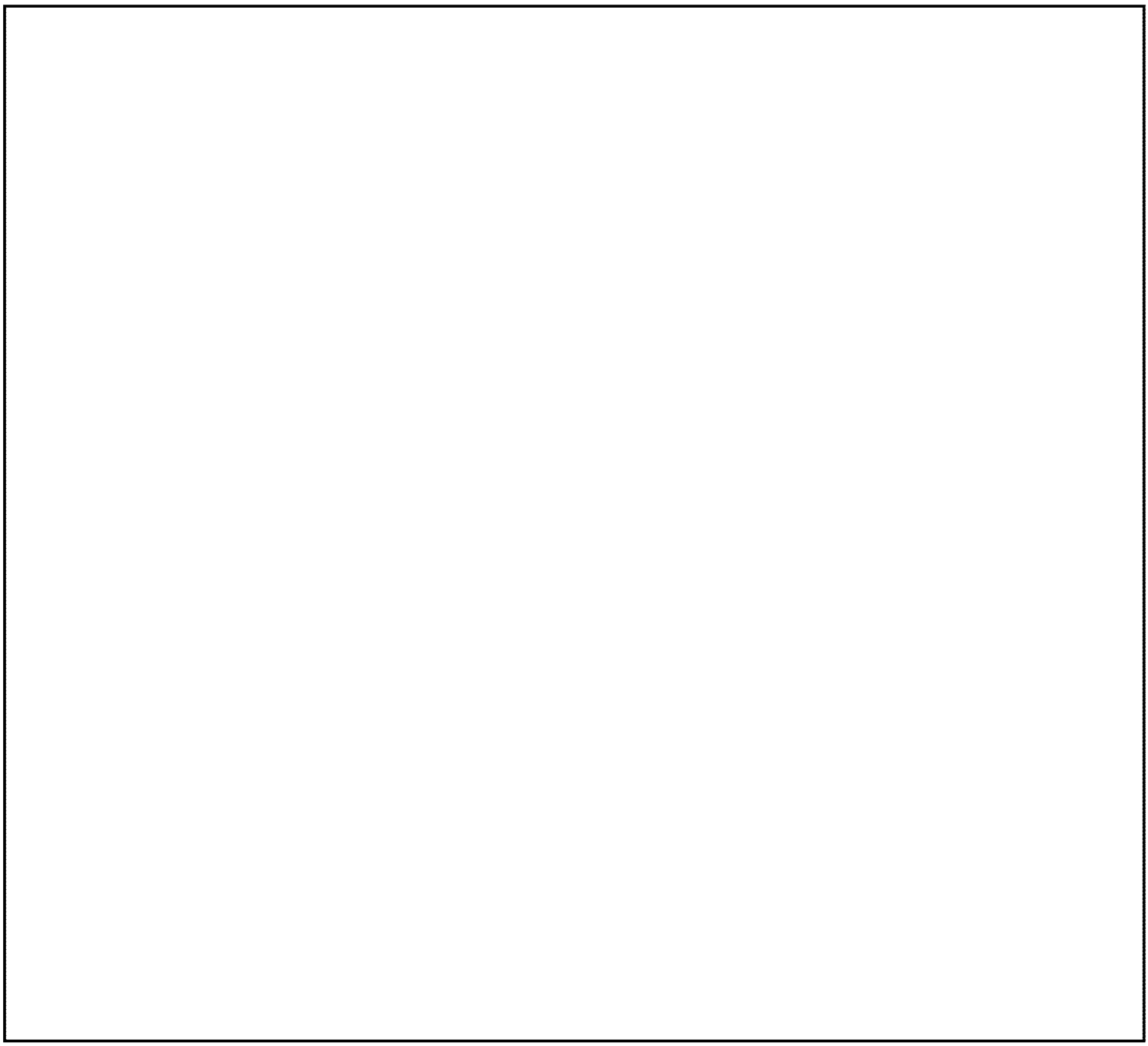




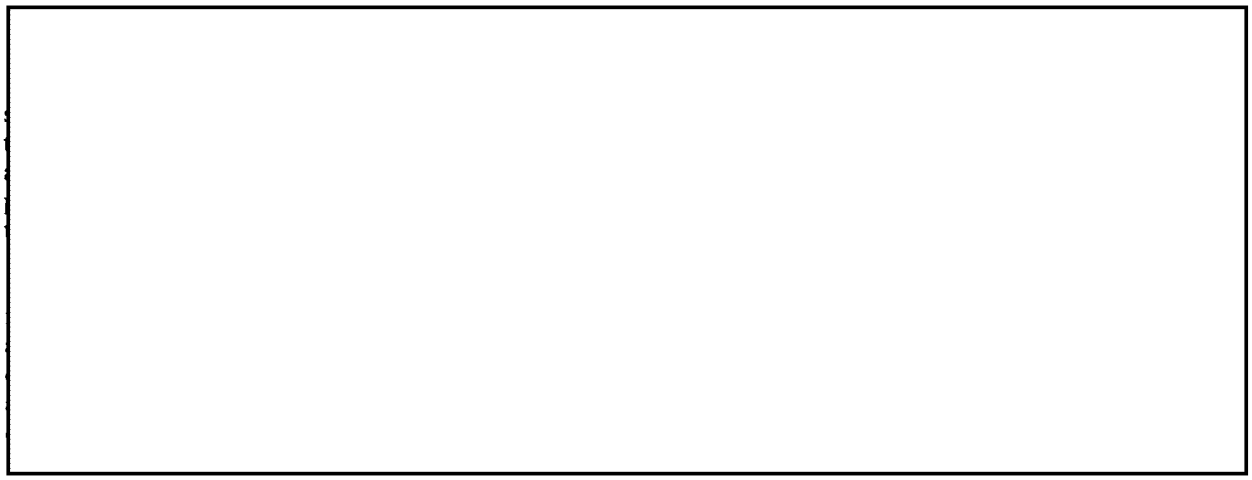
b5

b5



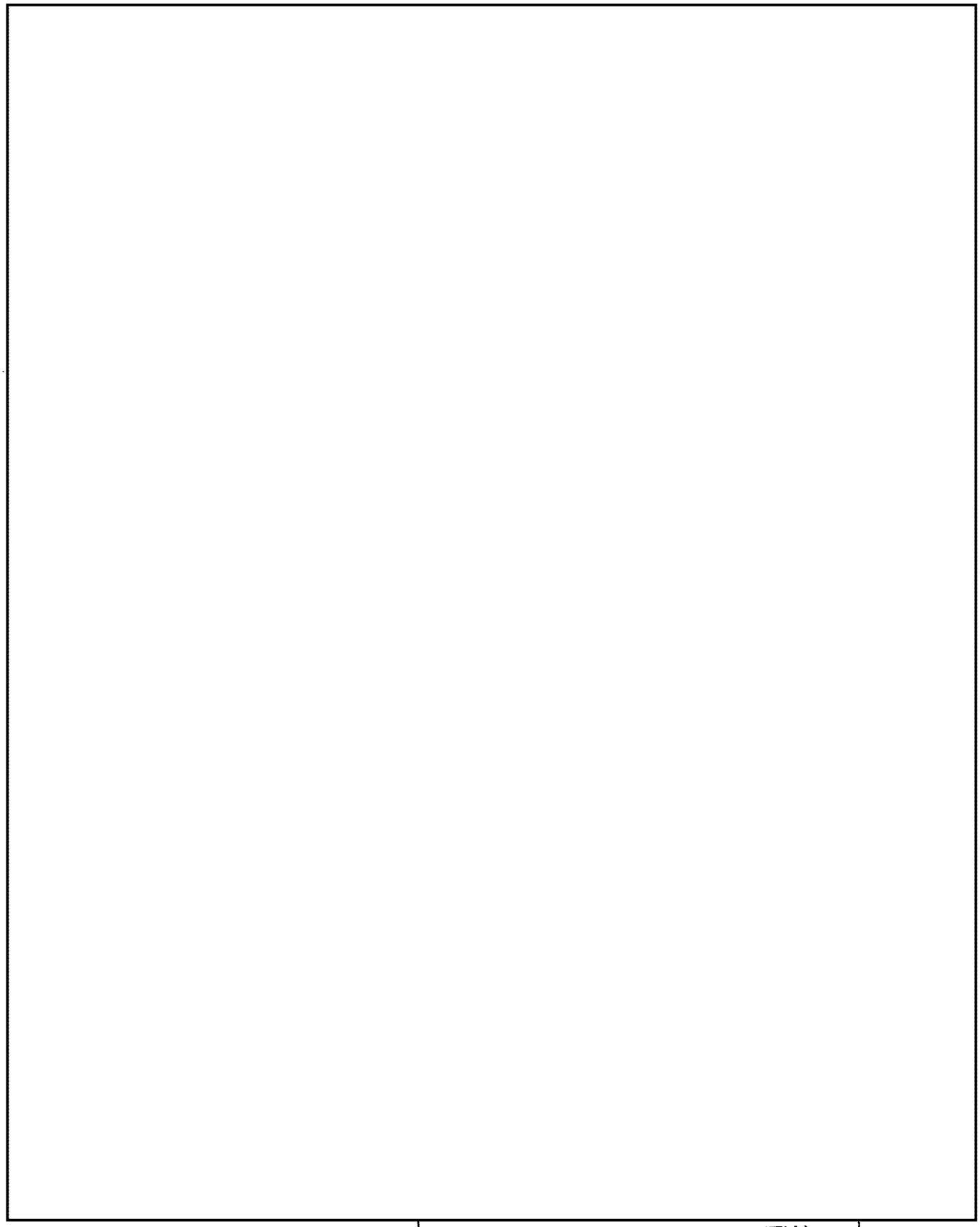


b5

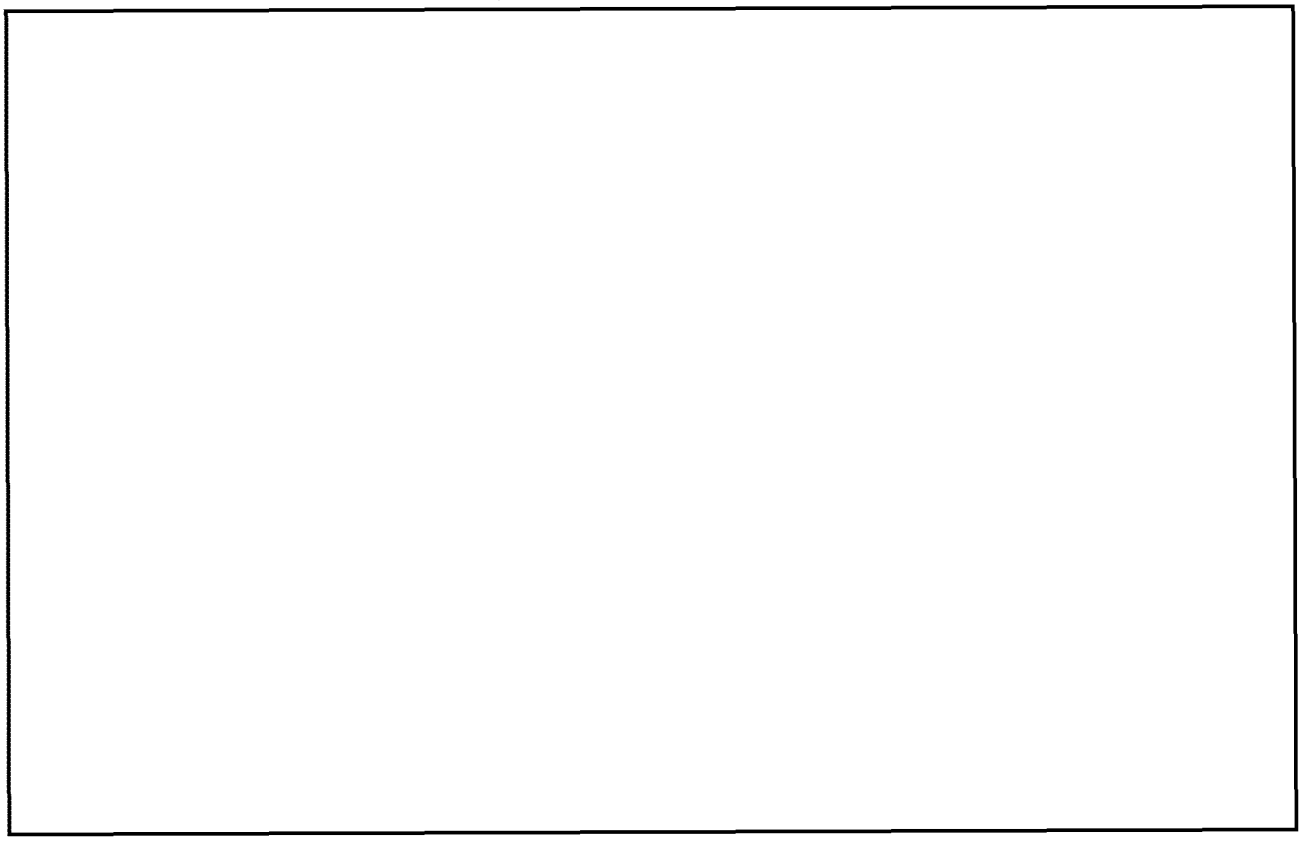


DRAFT – FOR OFFICIAL USE ONLY

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DRAFT: 4/19/04

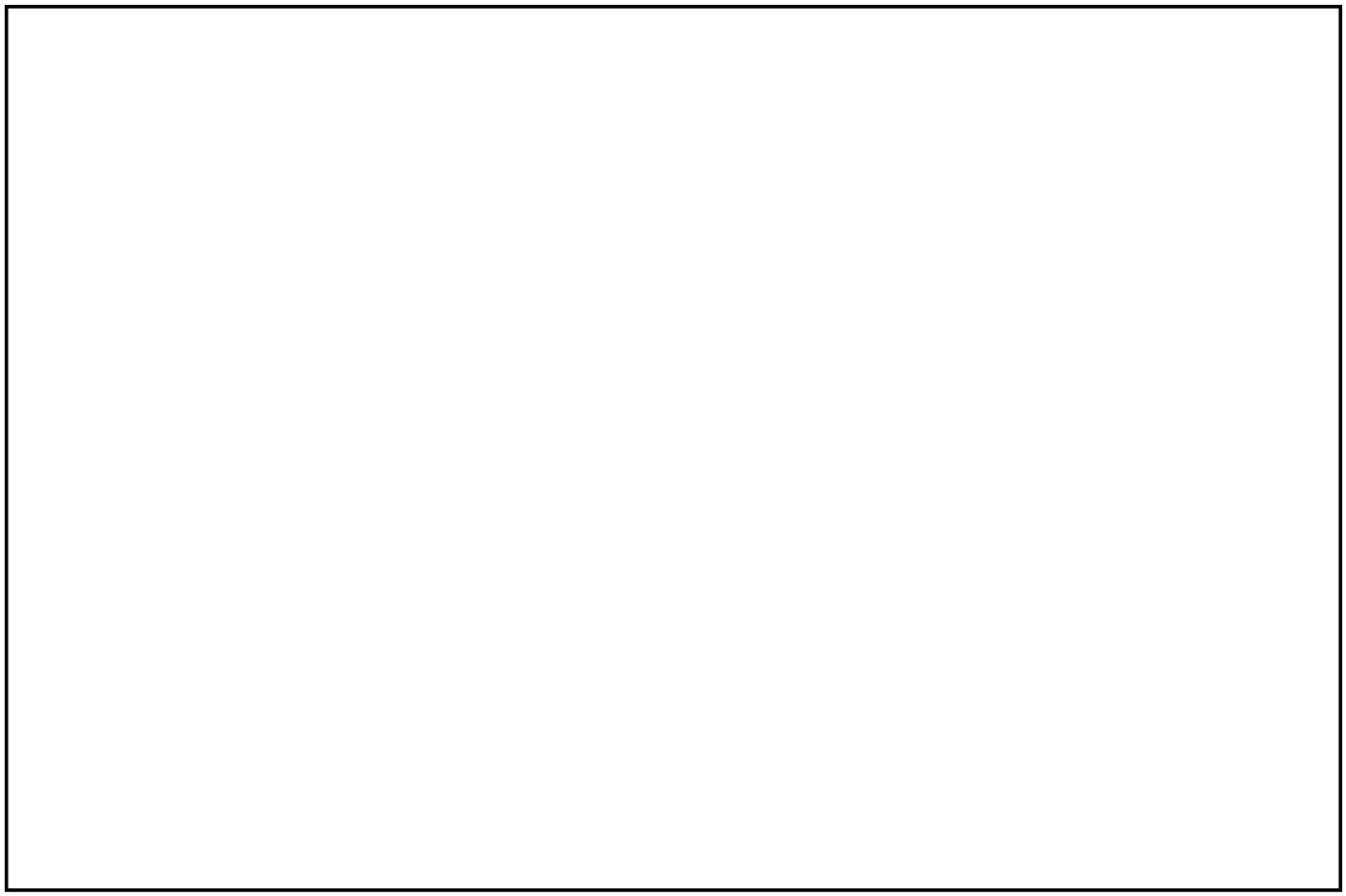
~~DATE: 10-12-2005~~
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 10-12-2030

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

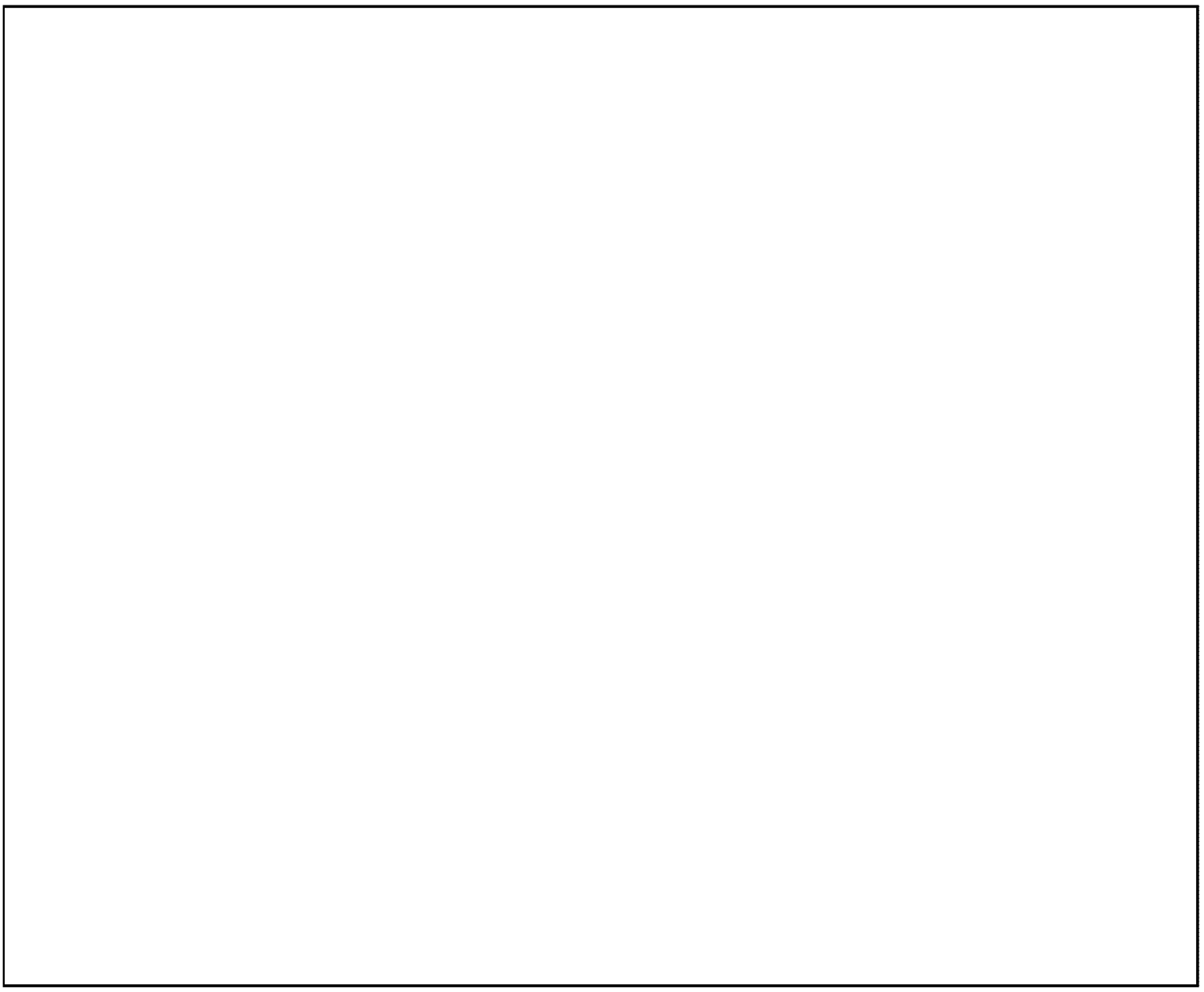
DATE: 12-05-2005
CLASSIFIED BY 65179/DMH/LP/DK
REASON: 1.4 ((C) 05-CV-0845)
DECLASSIFY ON: 12-05-2030

b5

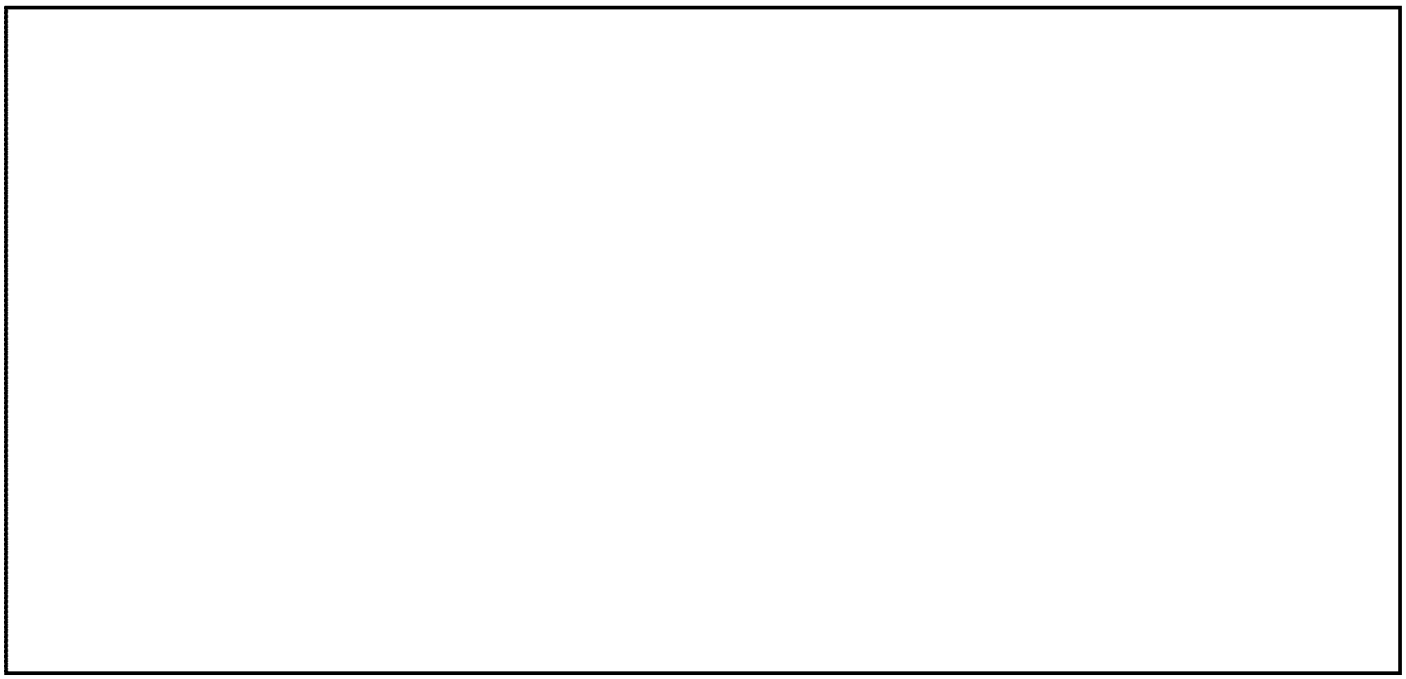


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

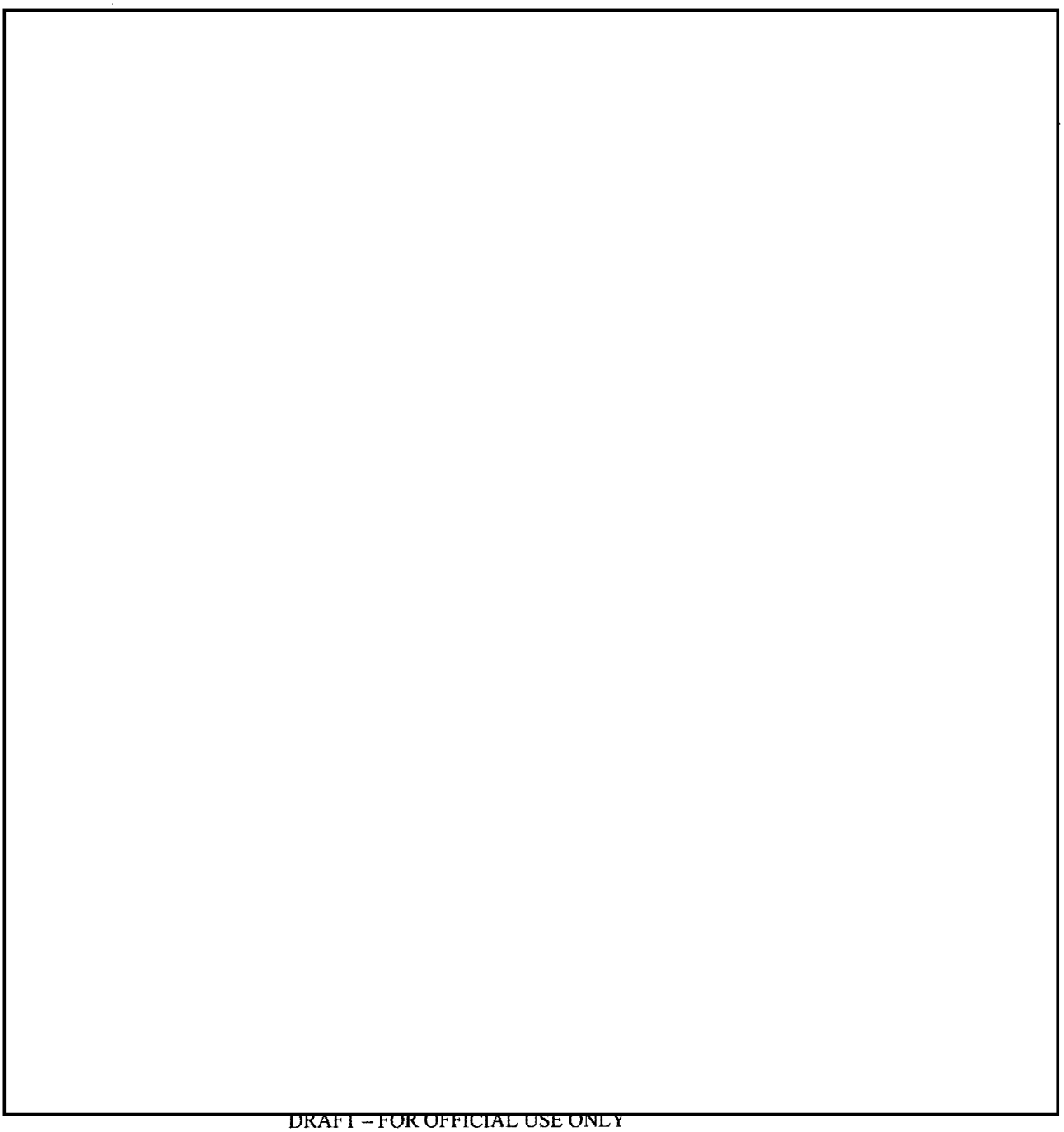


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

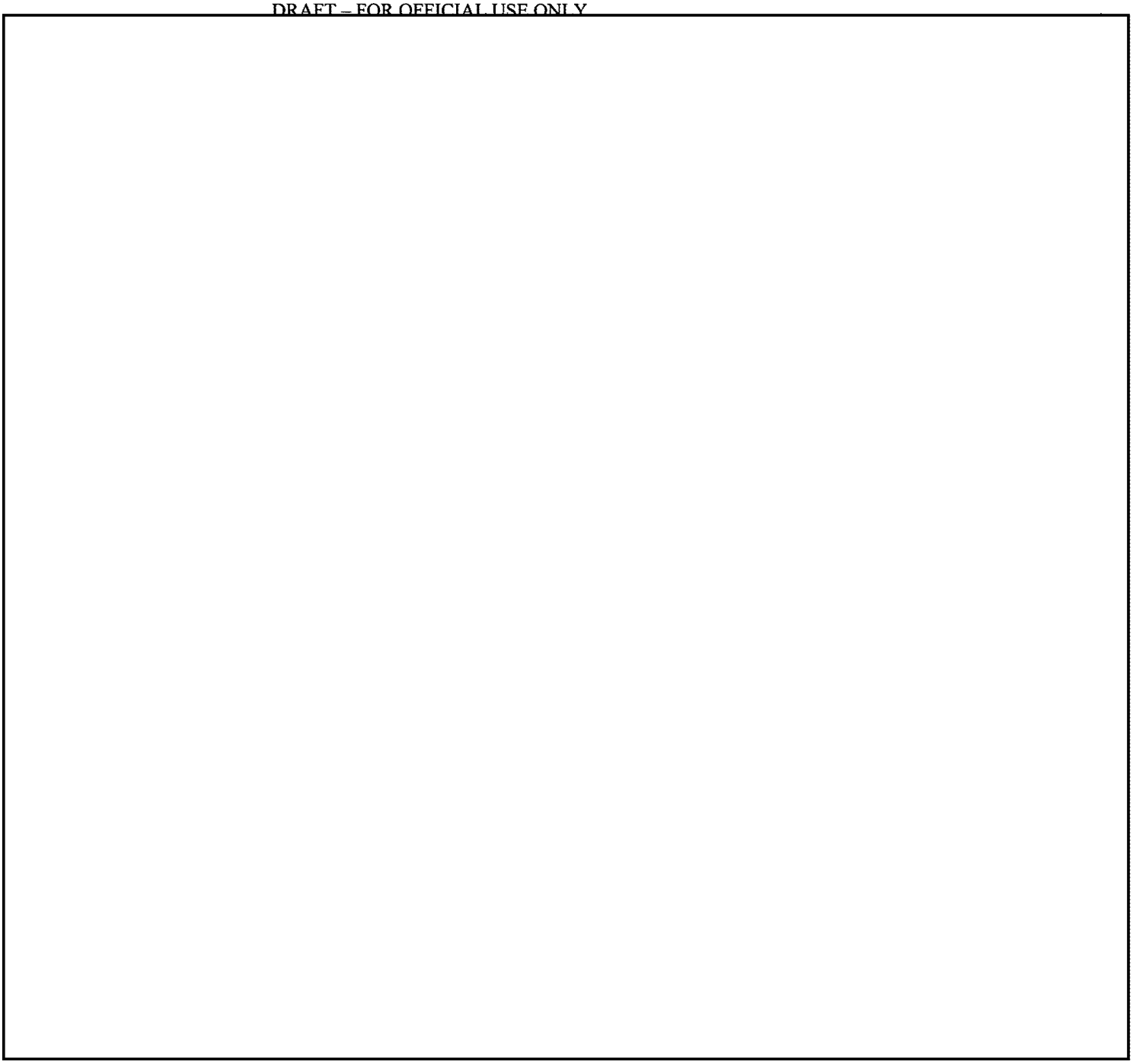


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

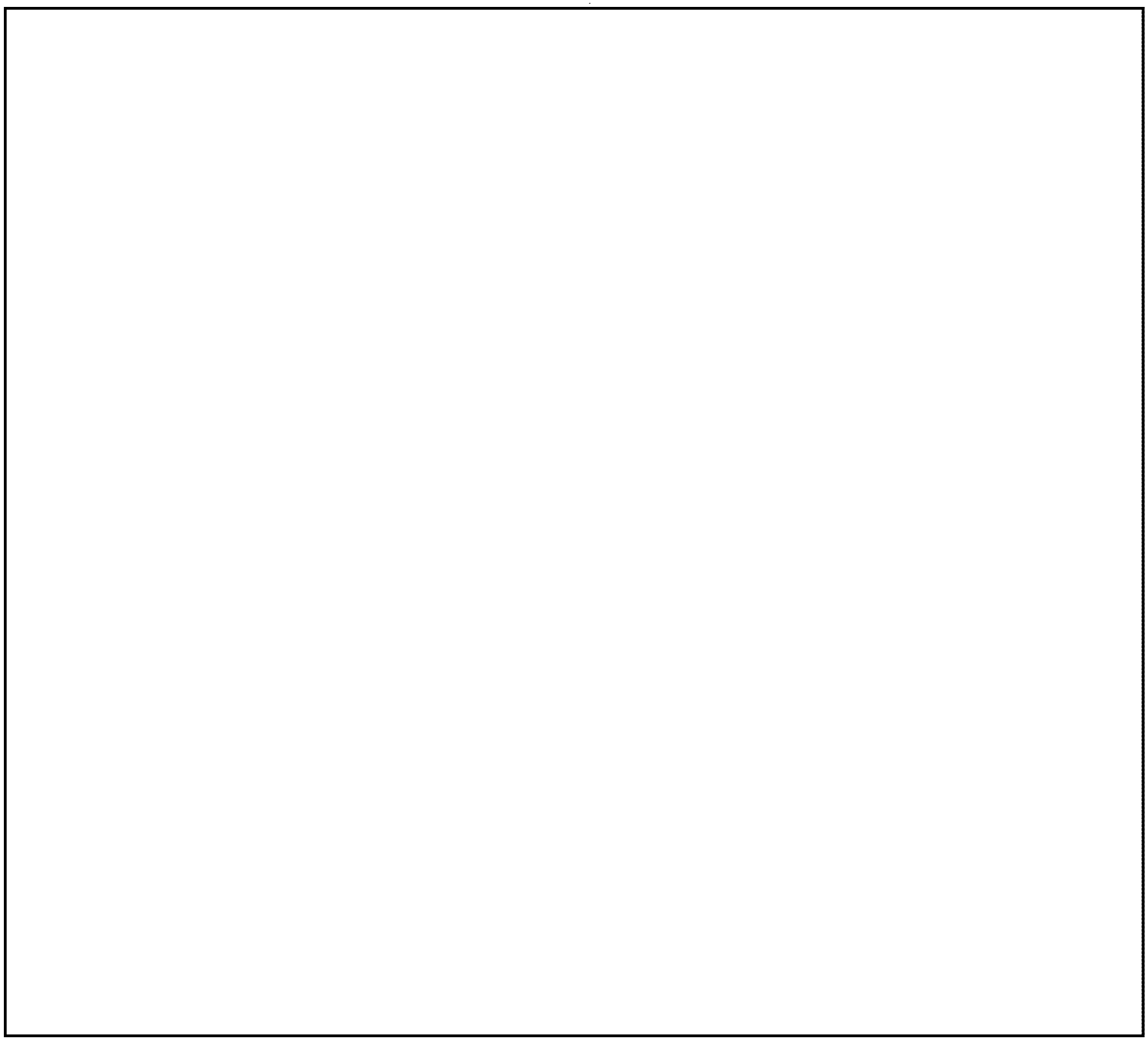
b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

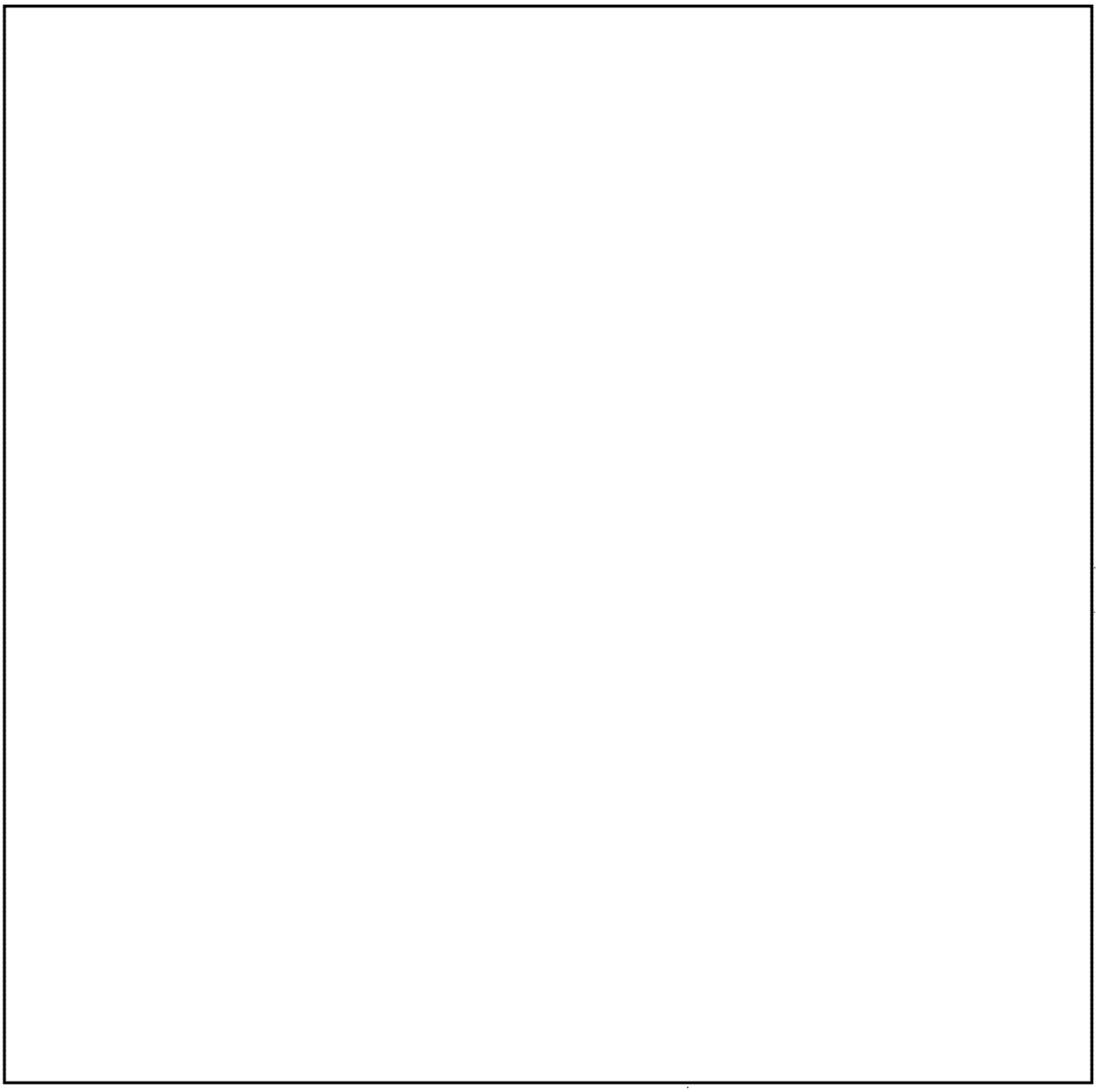
b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



b5

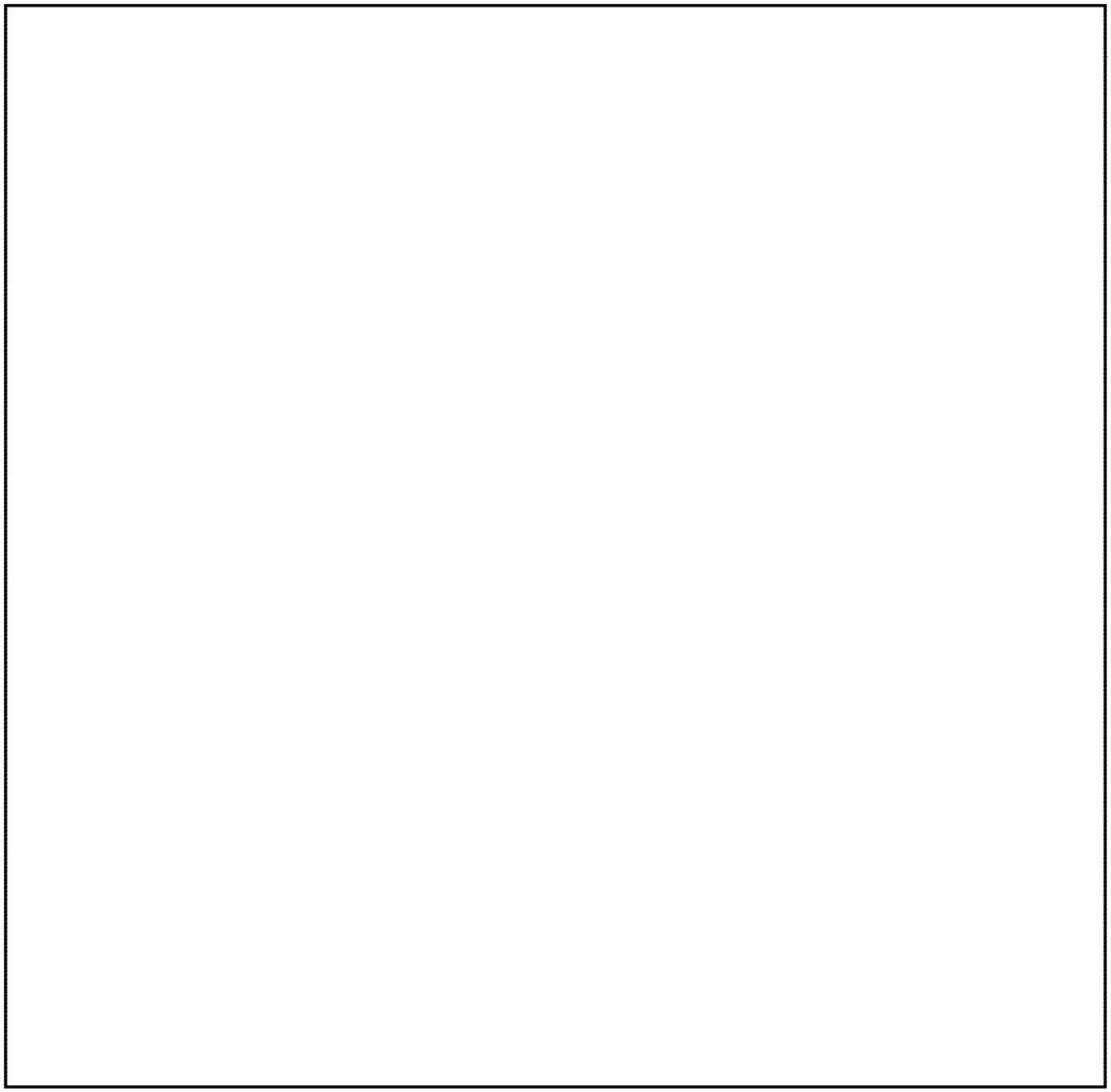


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

b5

b5



b5

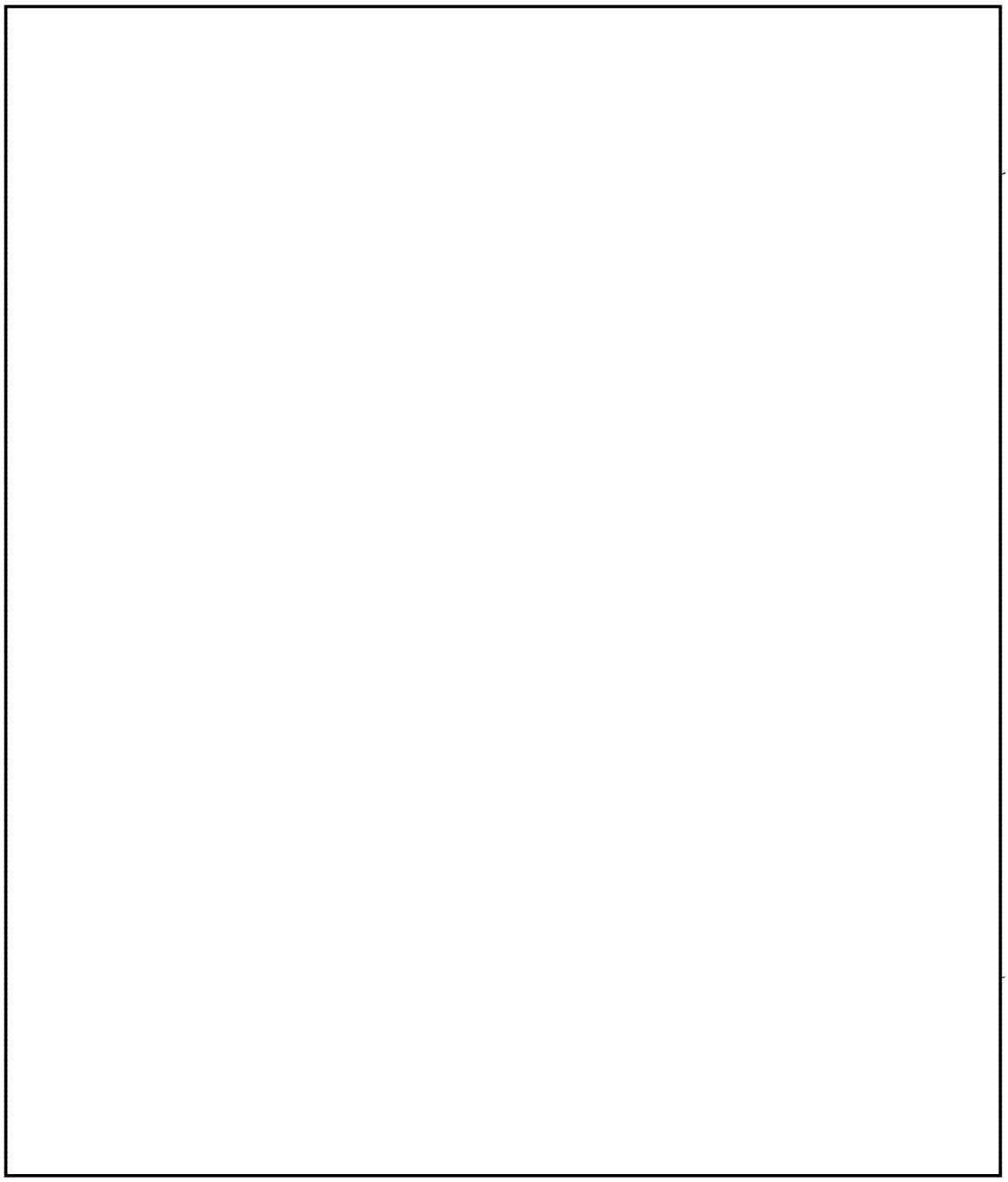
b5

b5

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

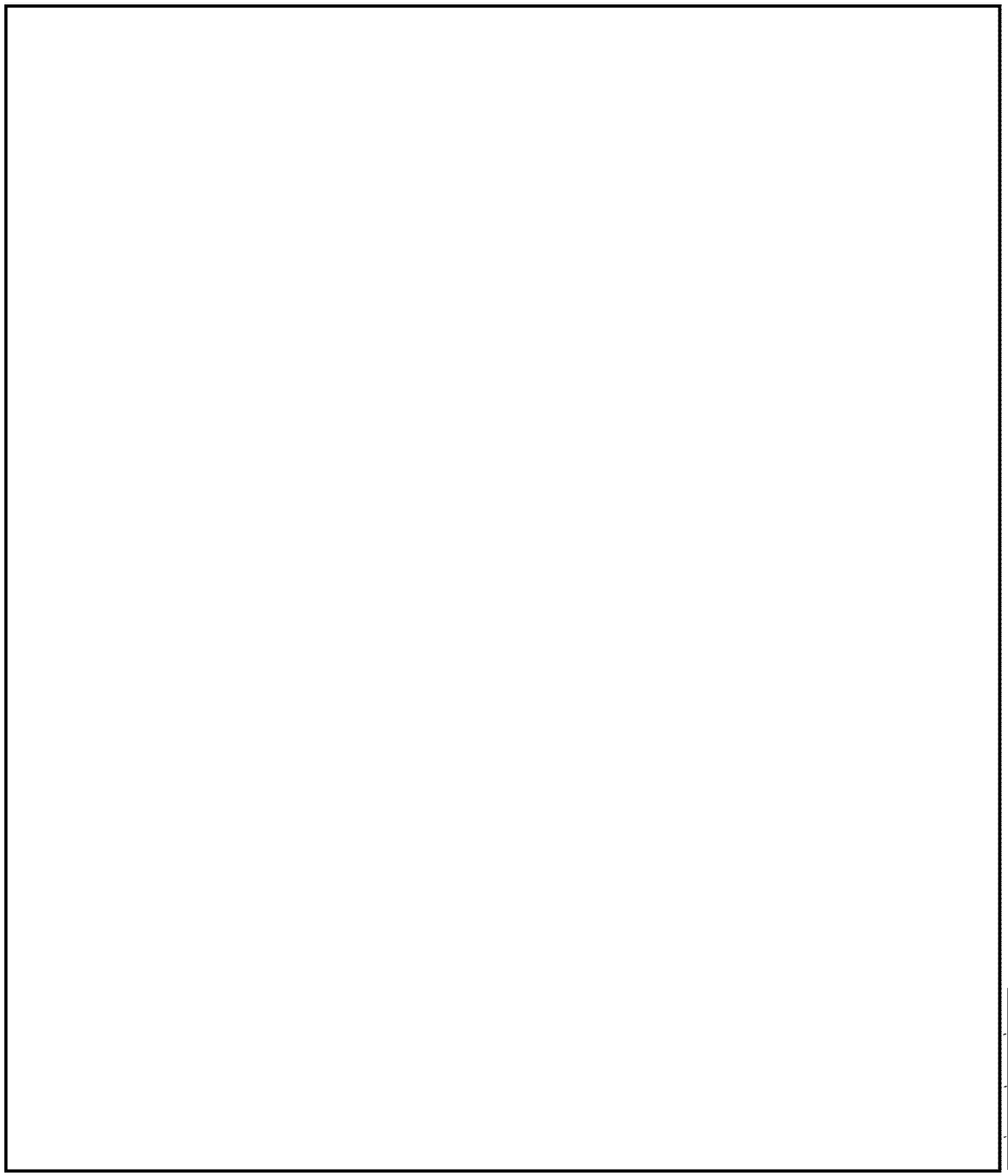
b5



b5

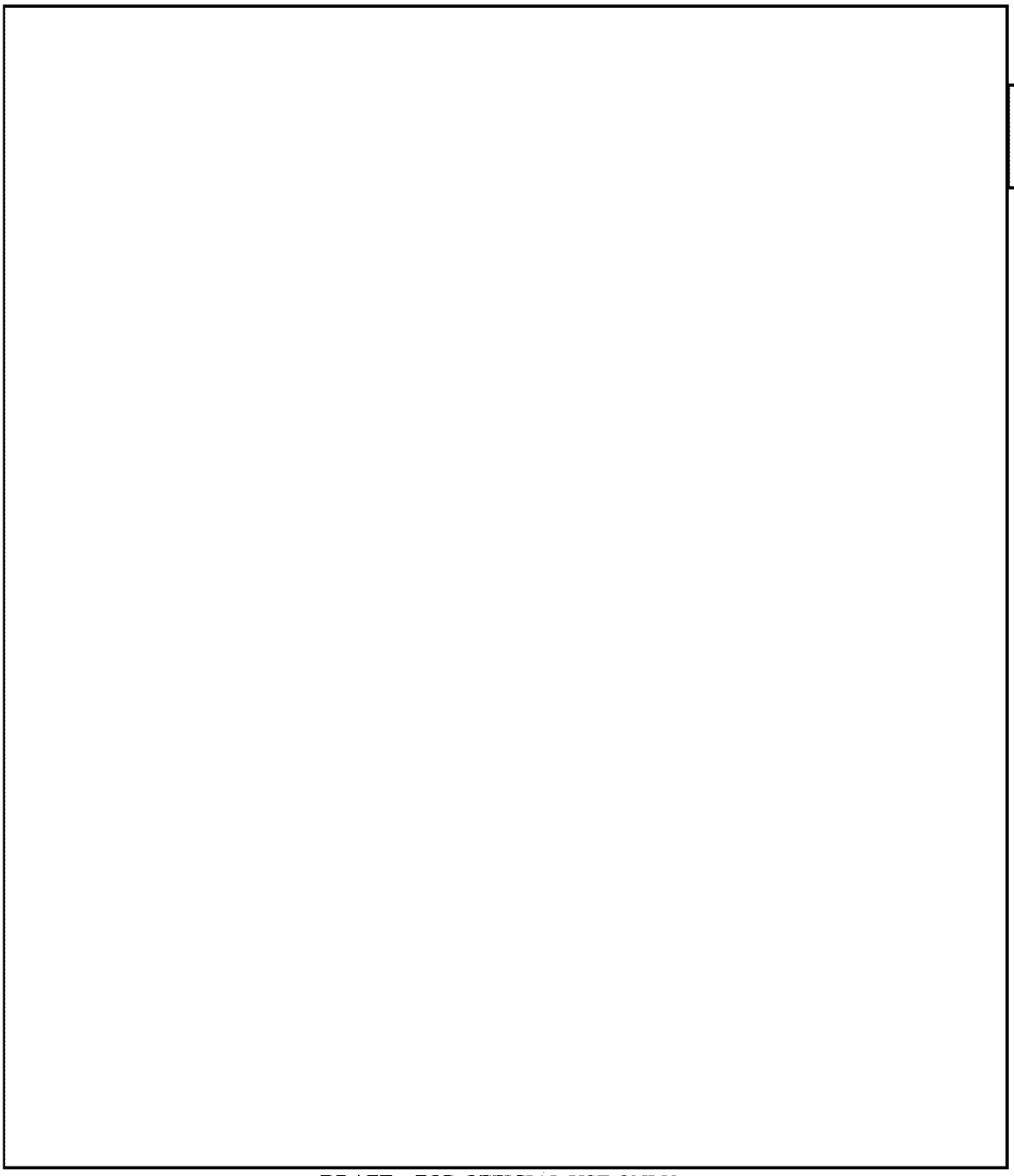
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



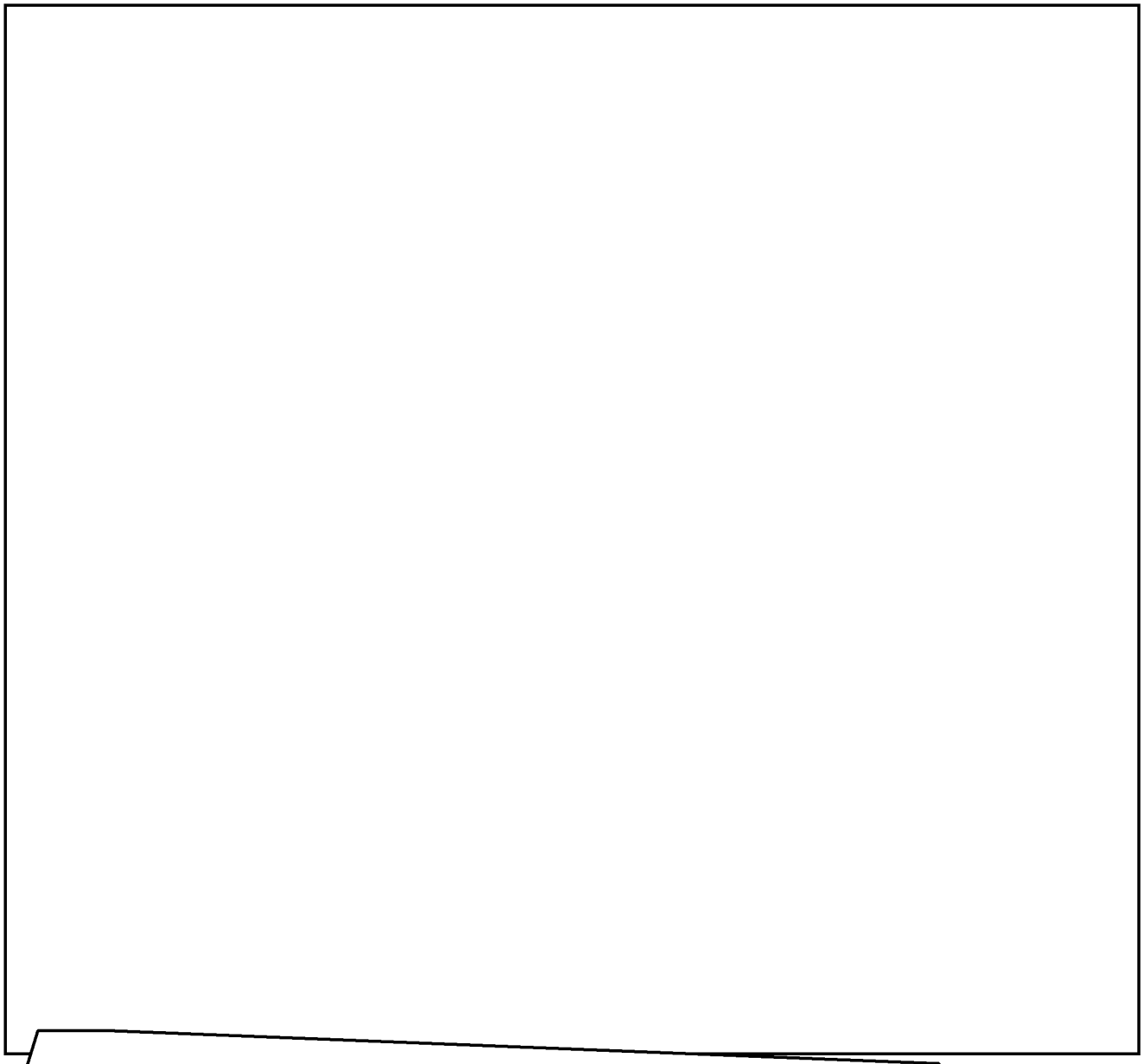
b5

b5



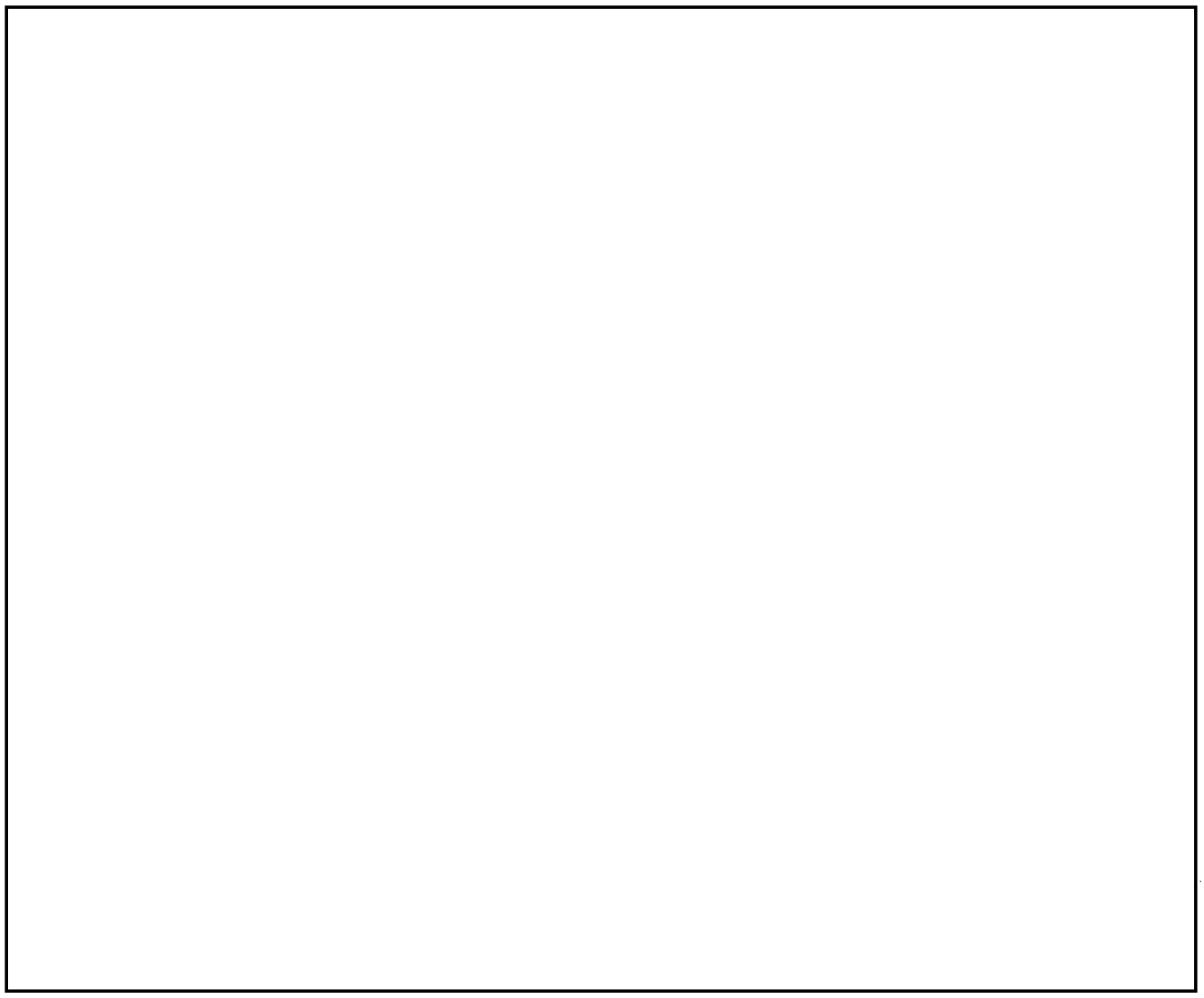
b5

b5



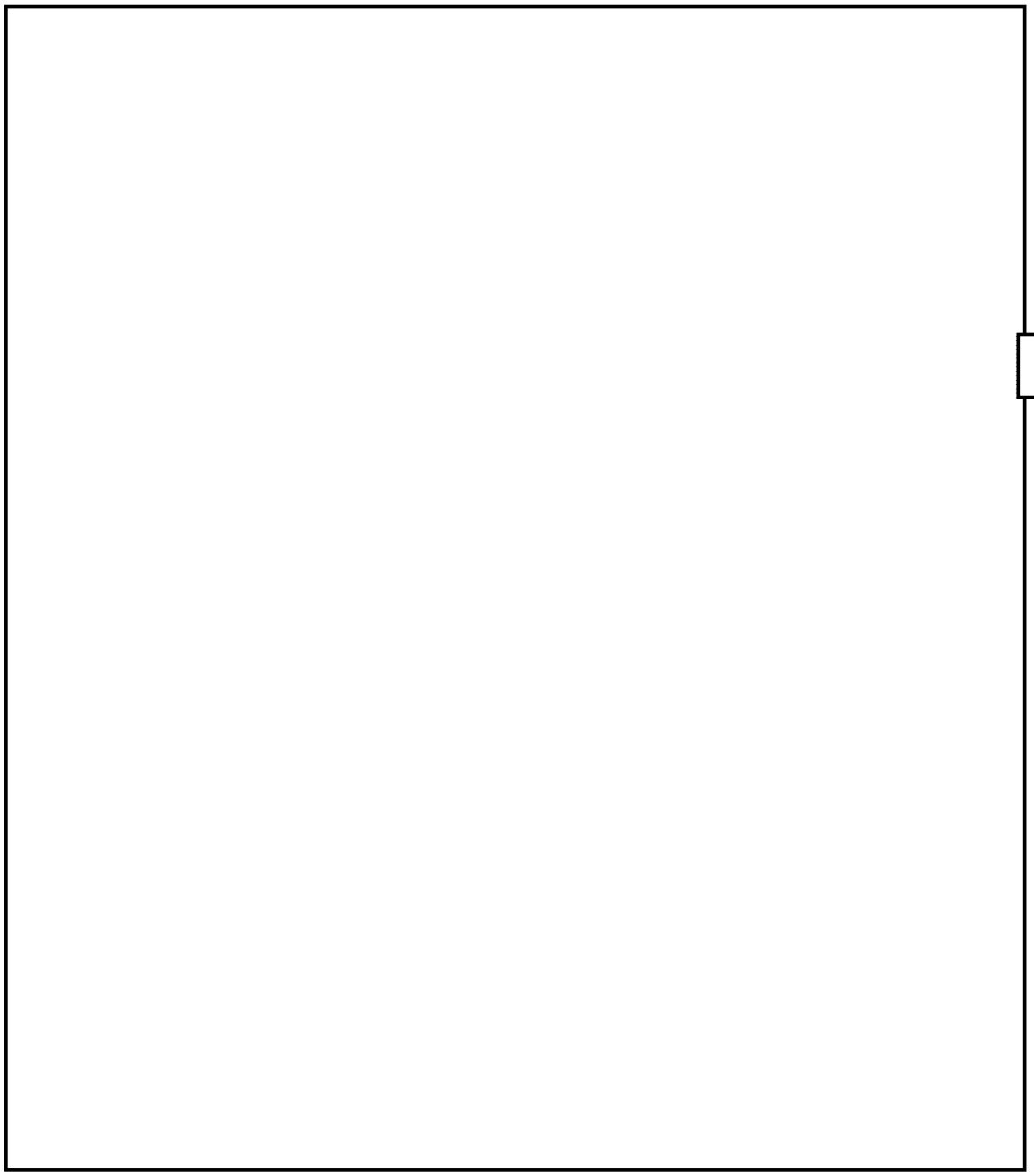
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

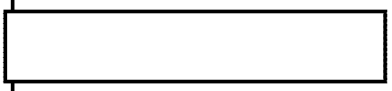


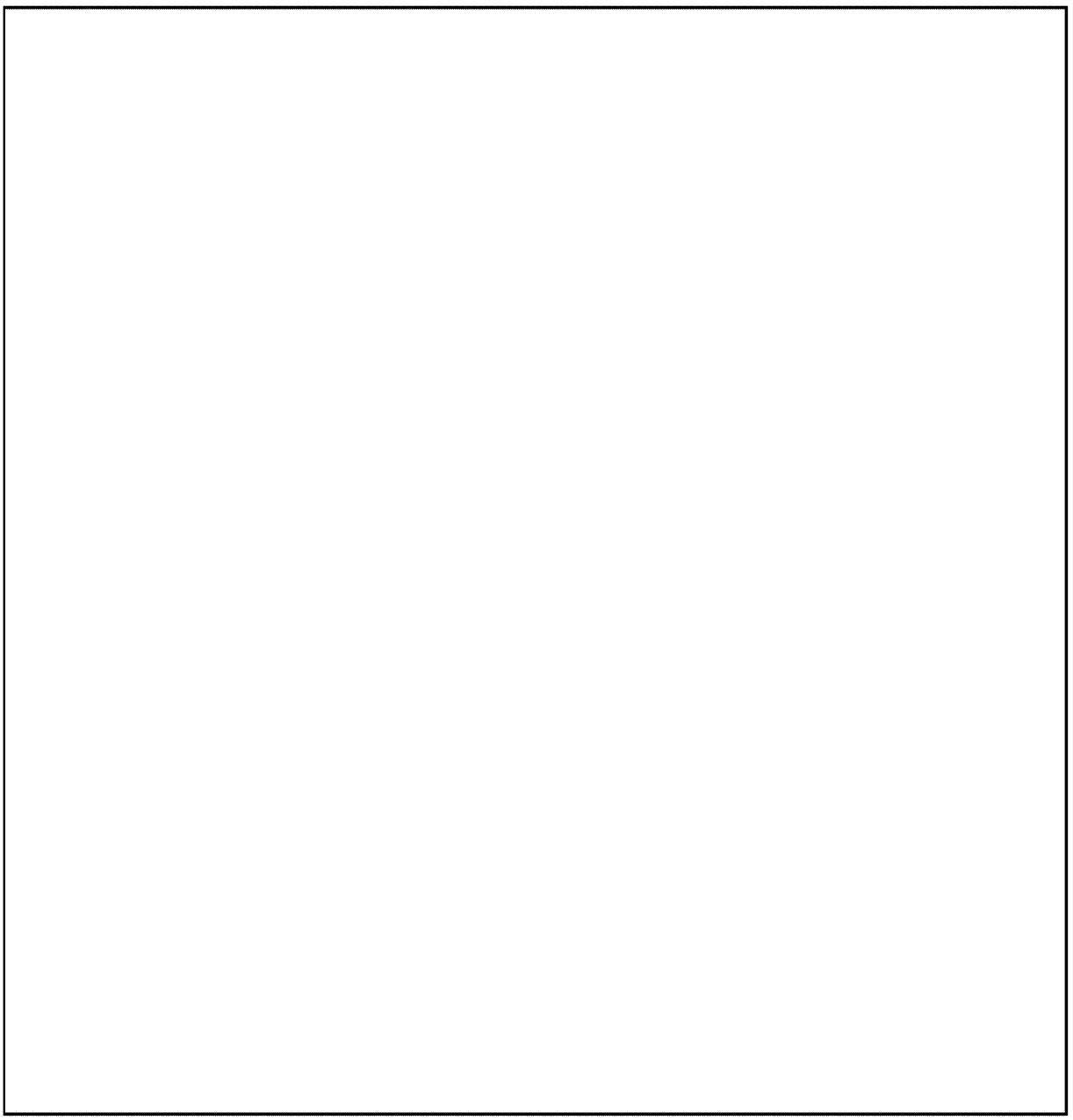
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



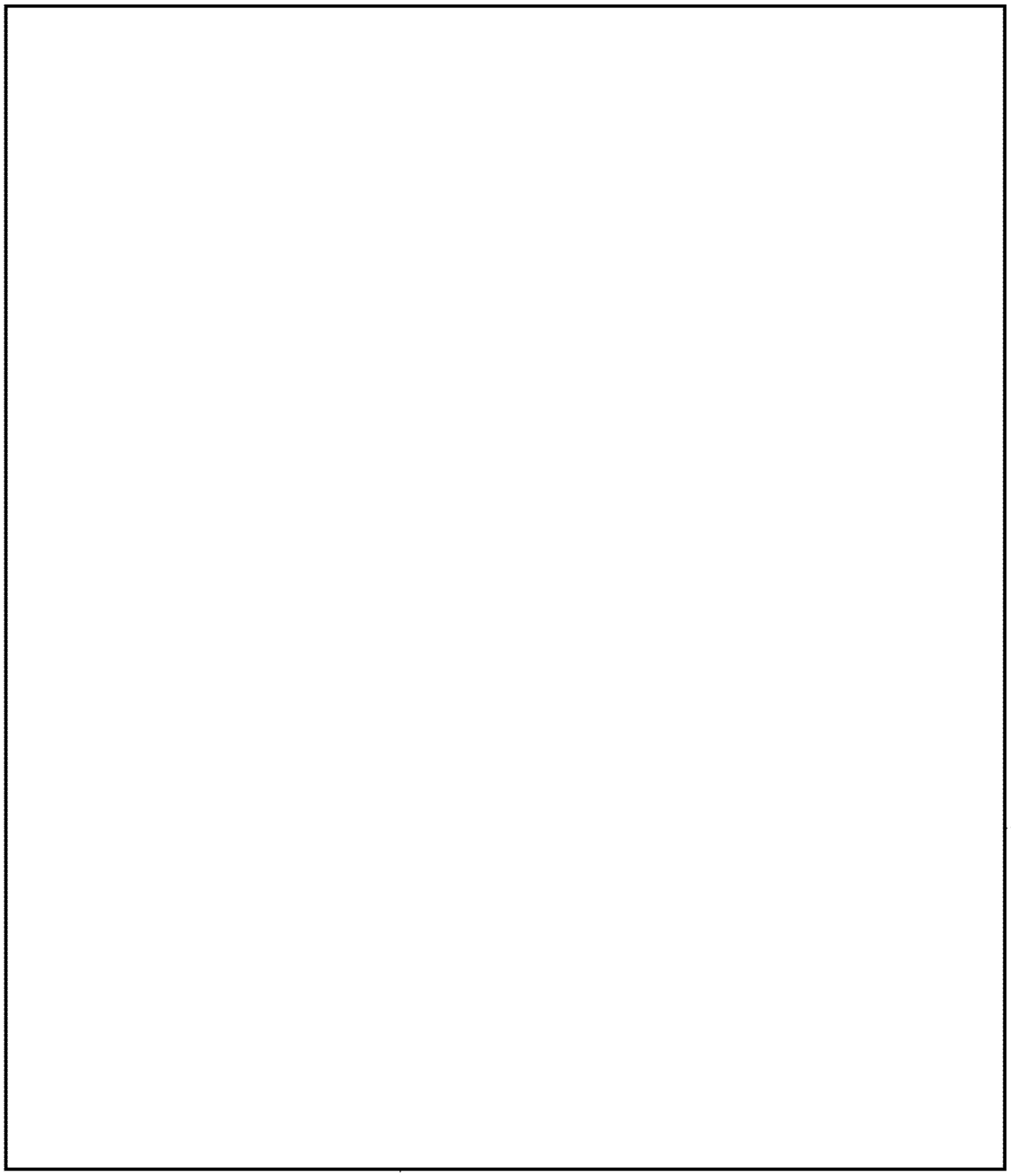
b5



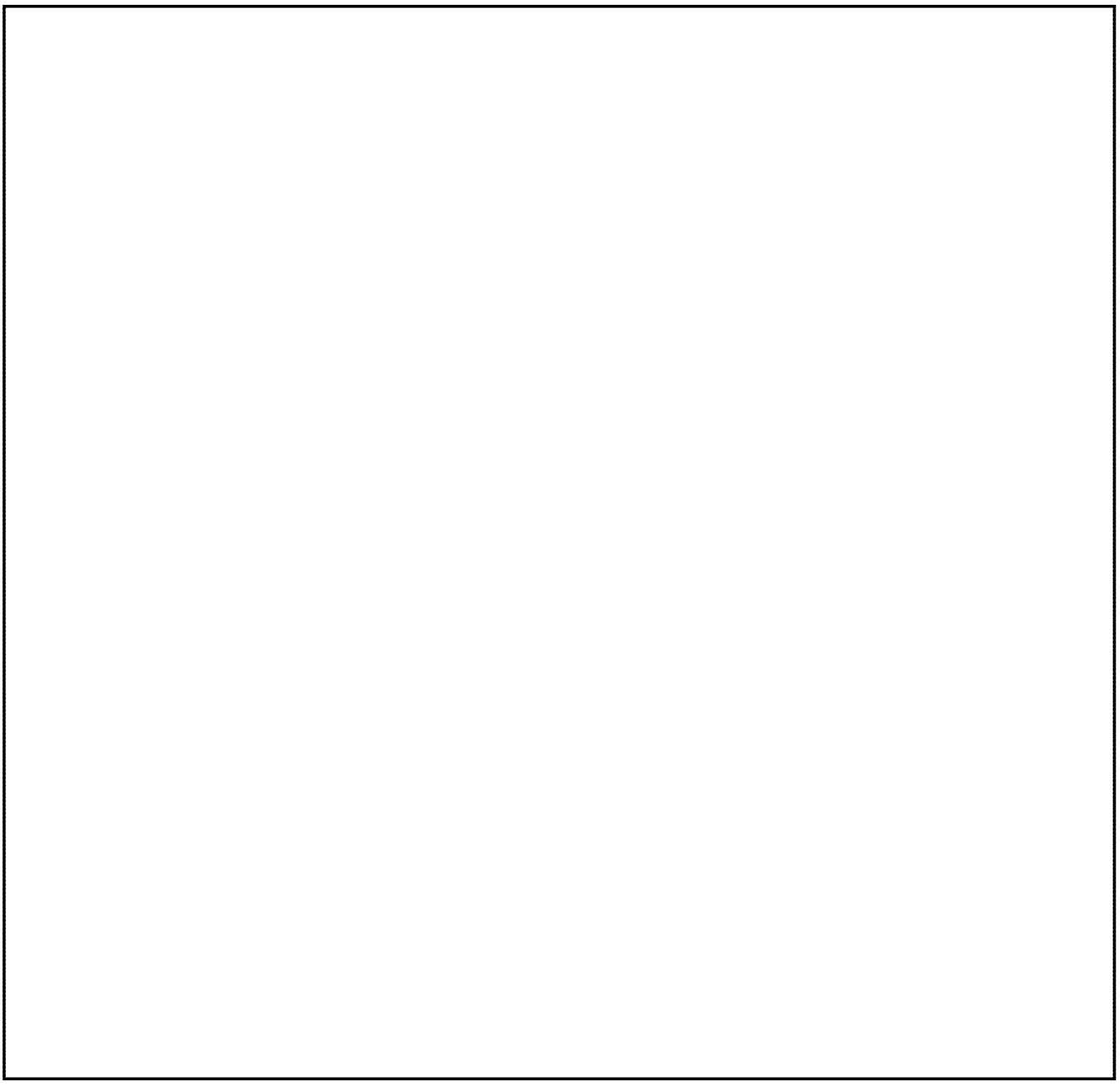


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

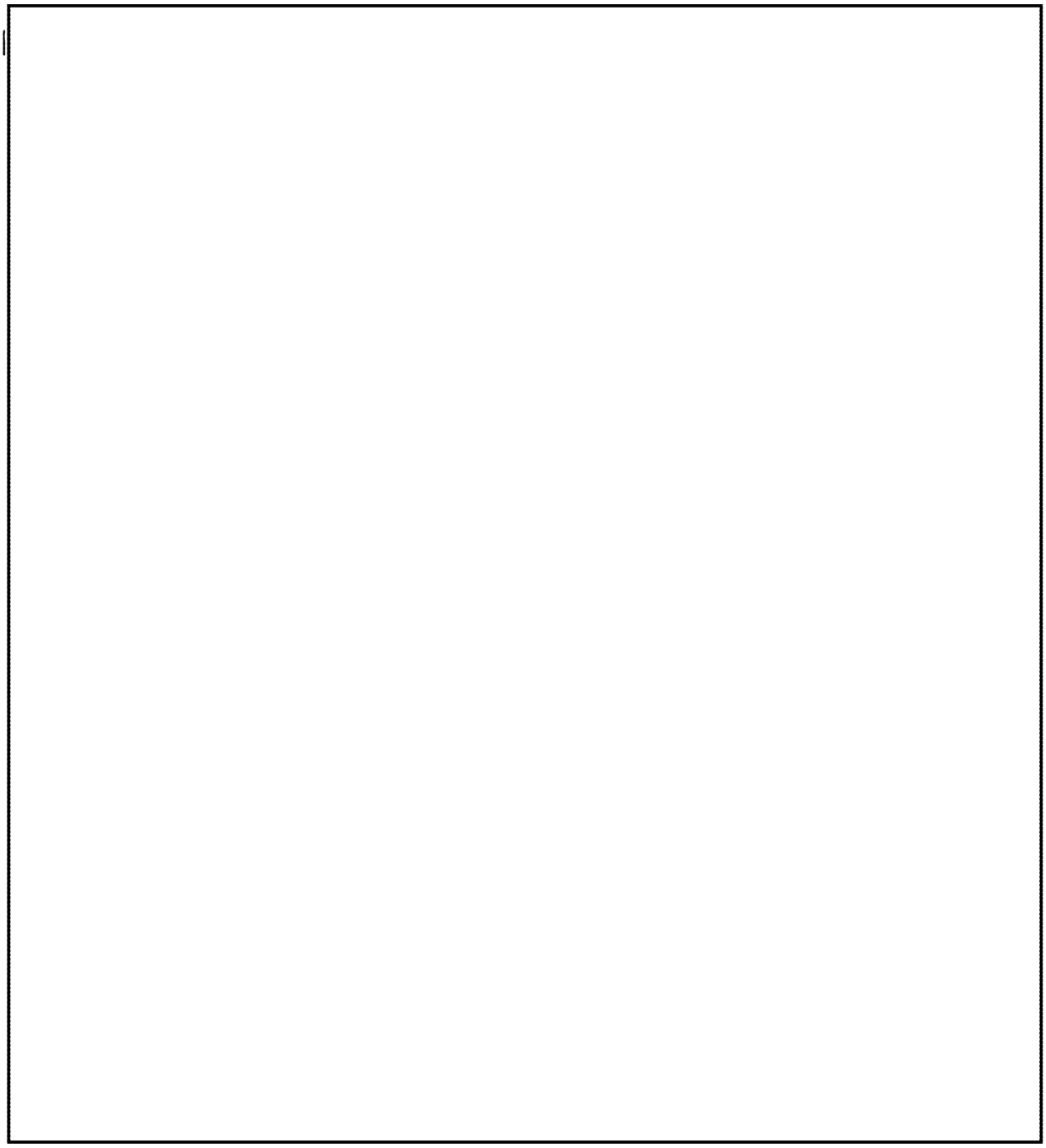
b5



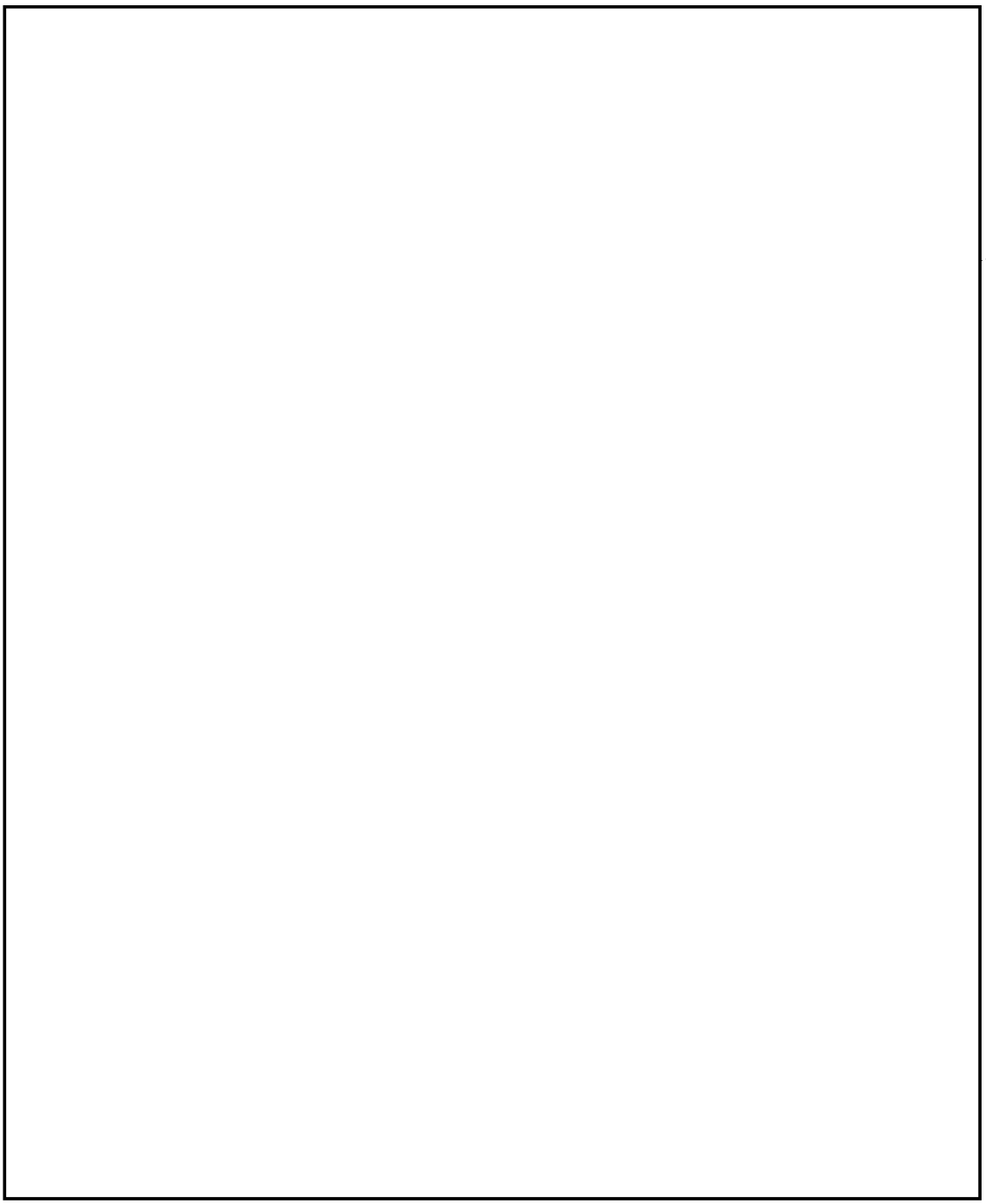
b5



b5



b5

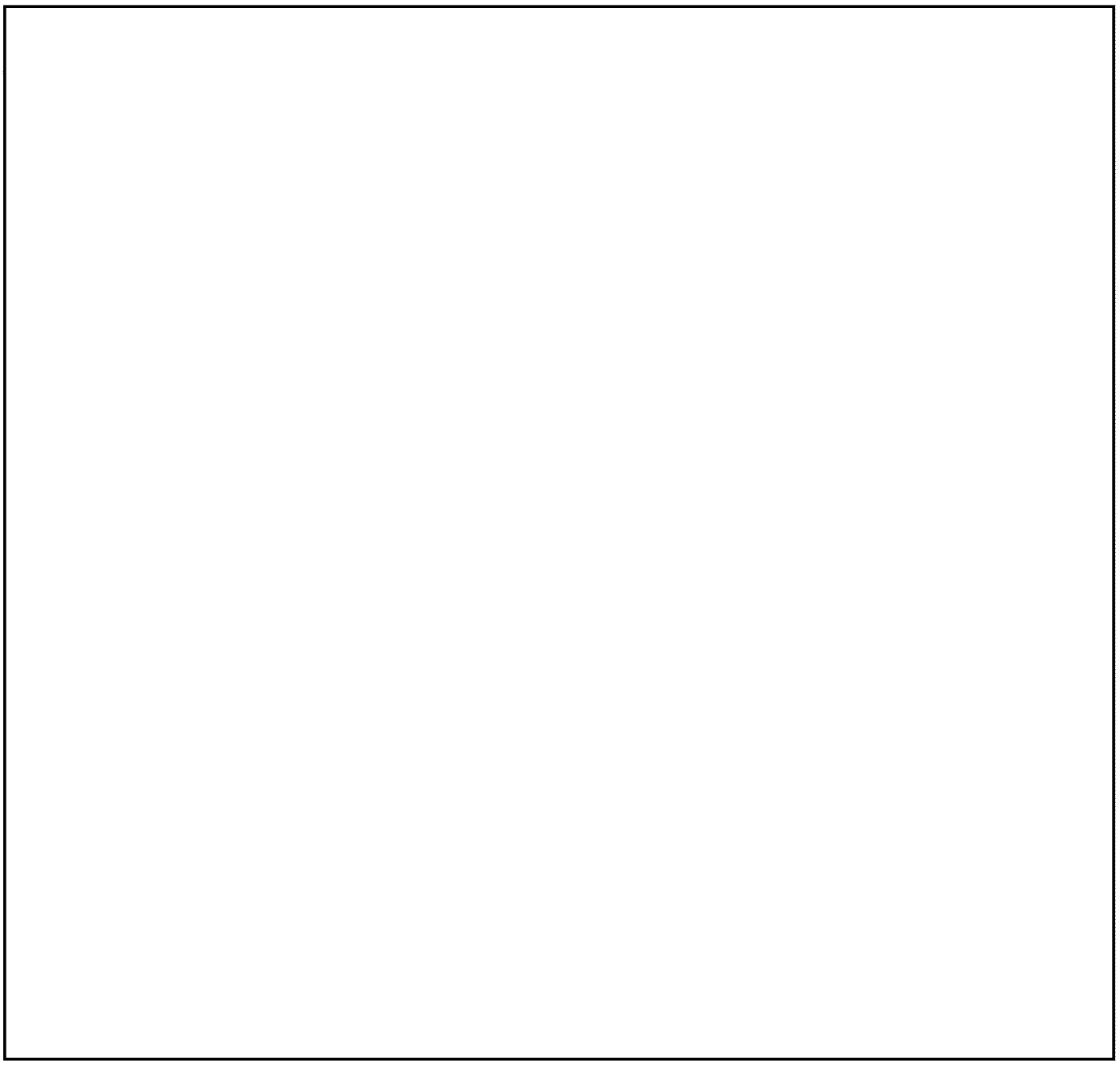


b5

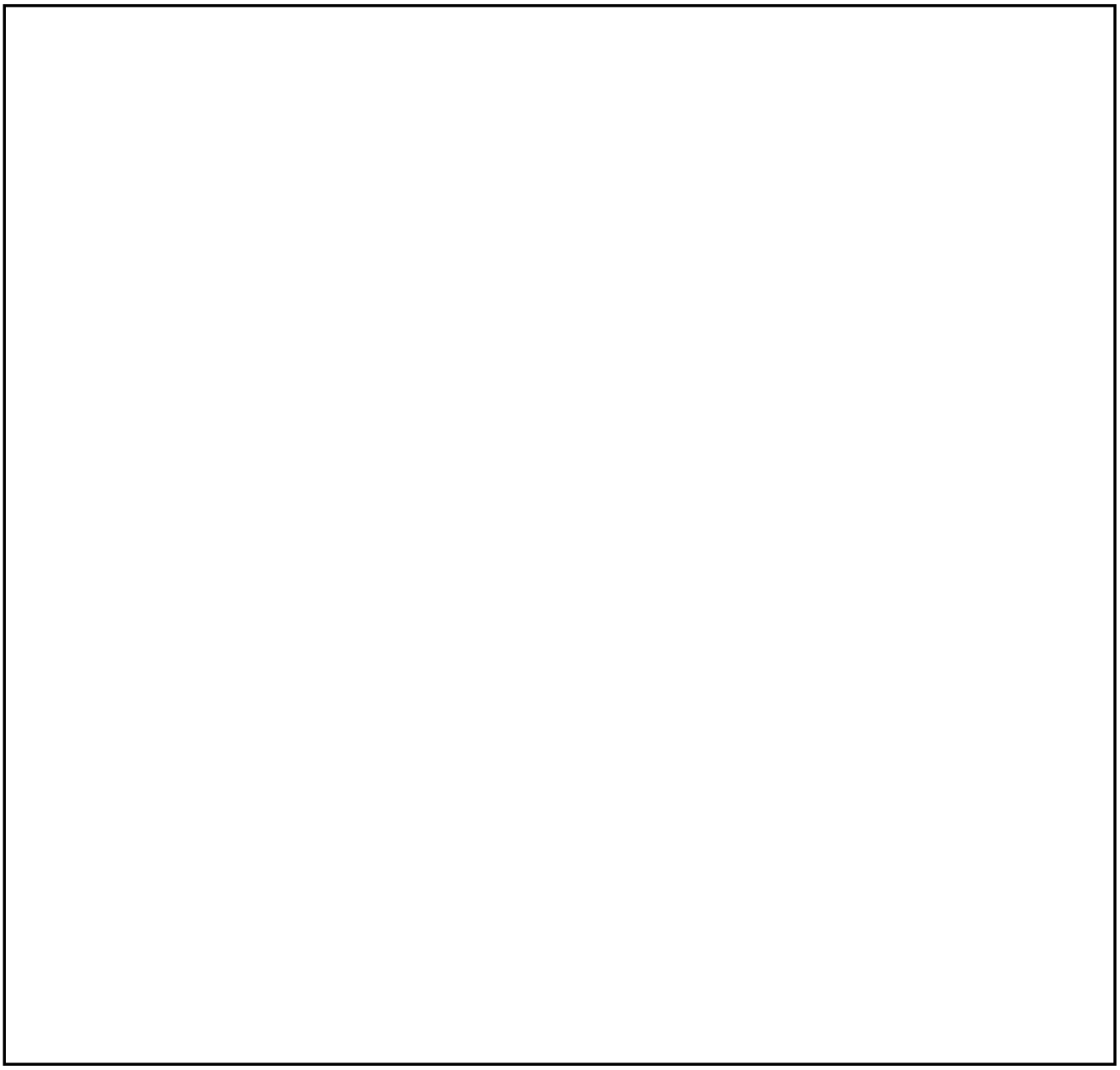
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT



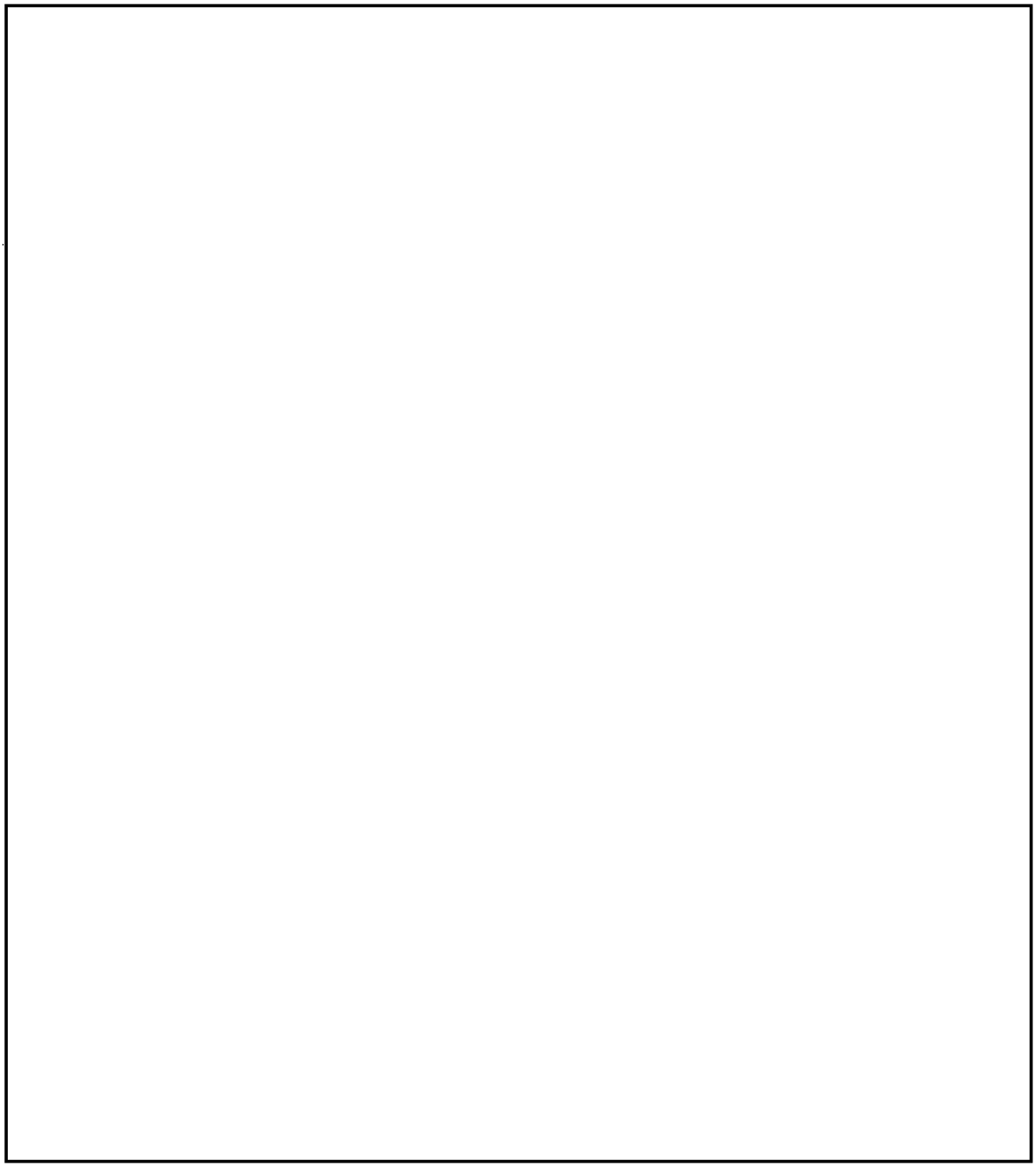
b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

DRAFT – FOR OFFICIAL USE ONLY

b5

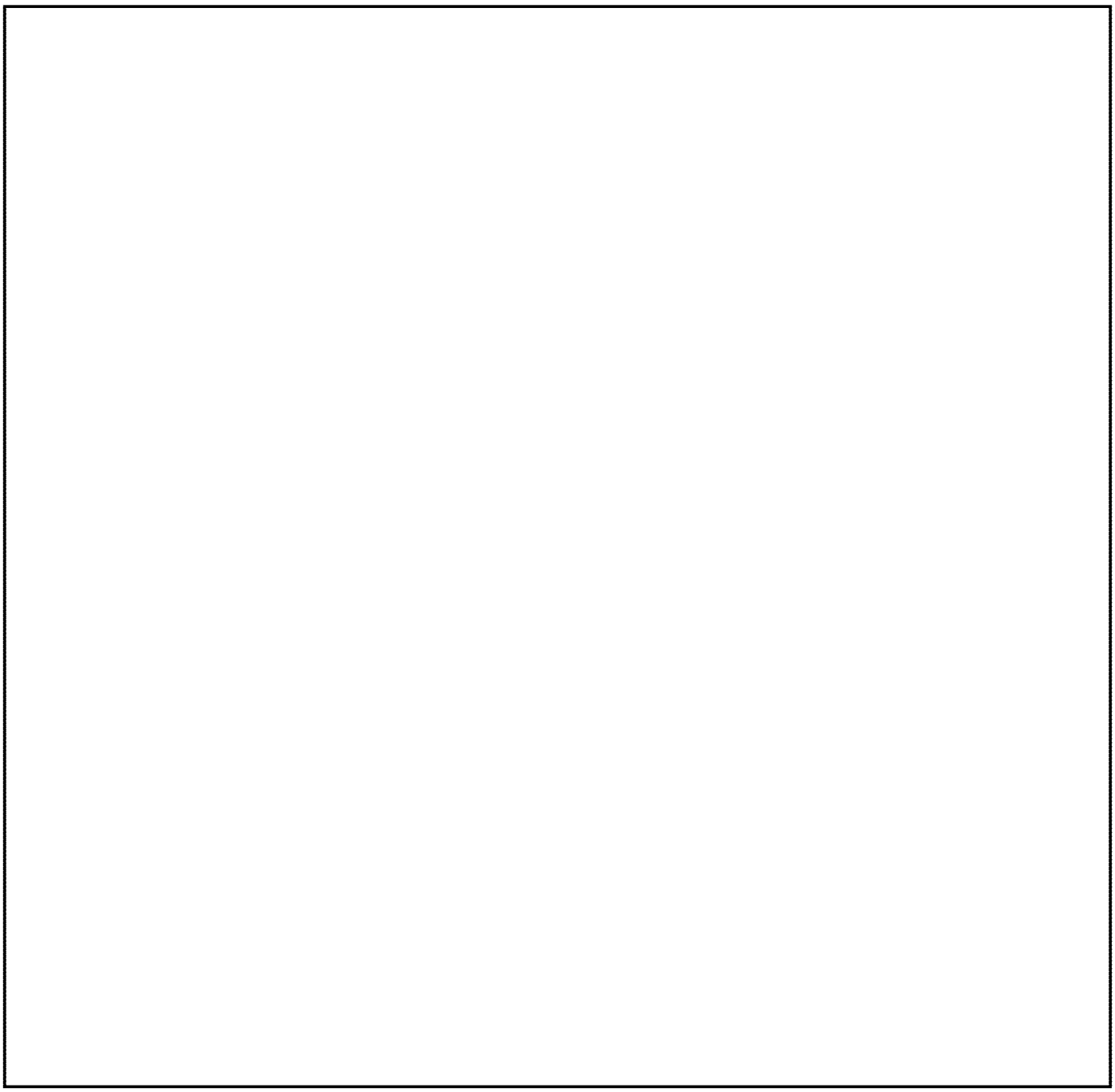


DRAFT – FOR OFFICIAL USE ONLY

SECRET

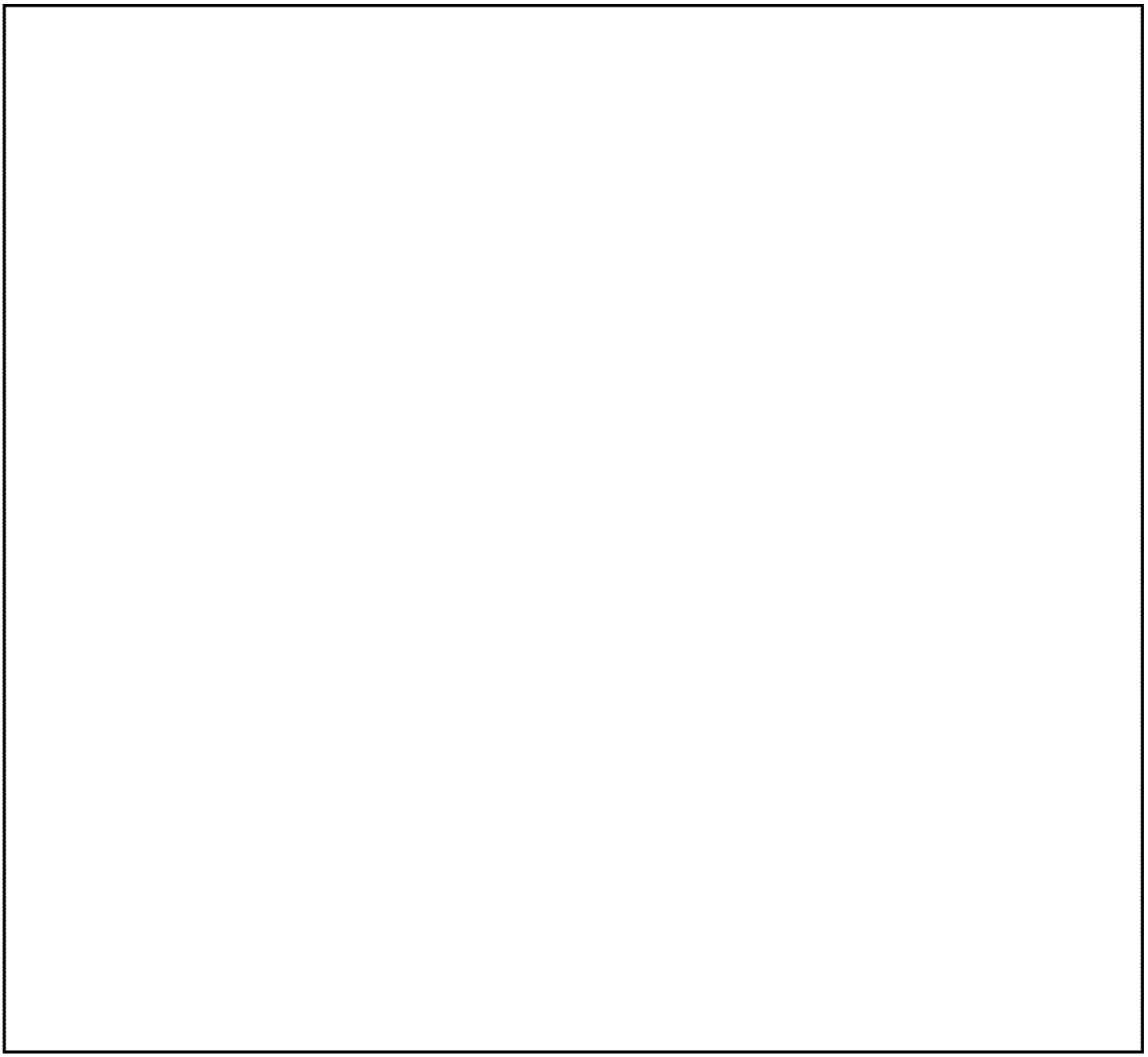
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



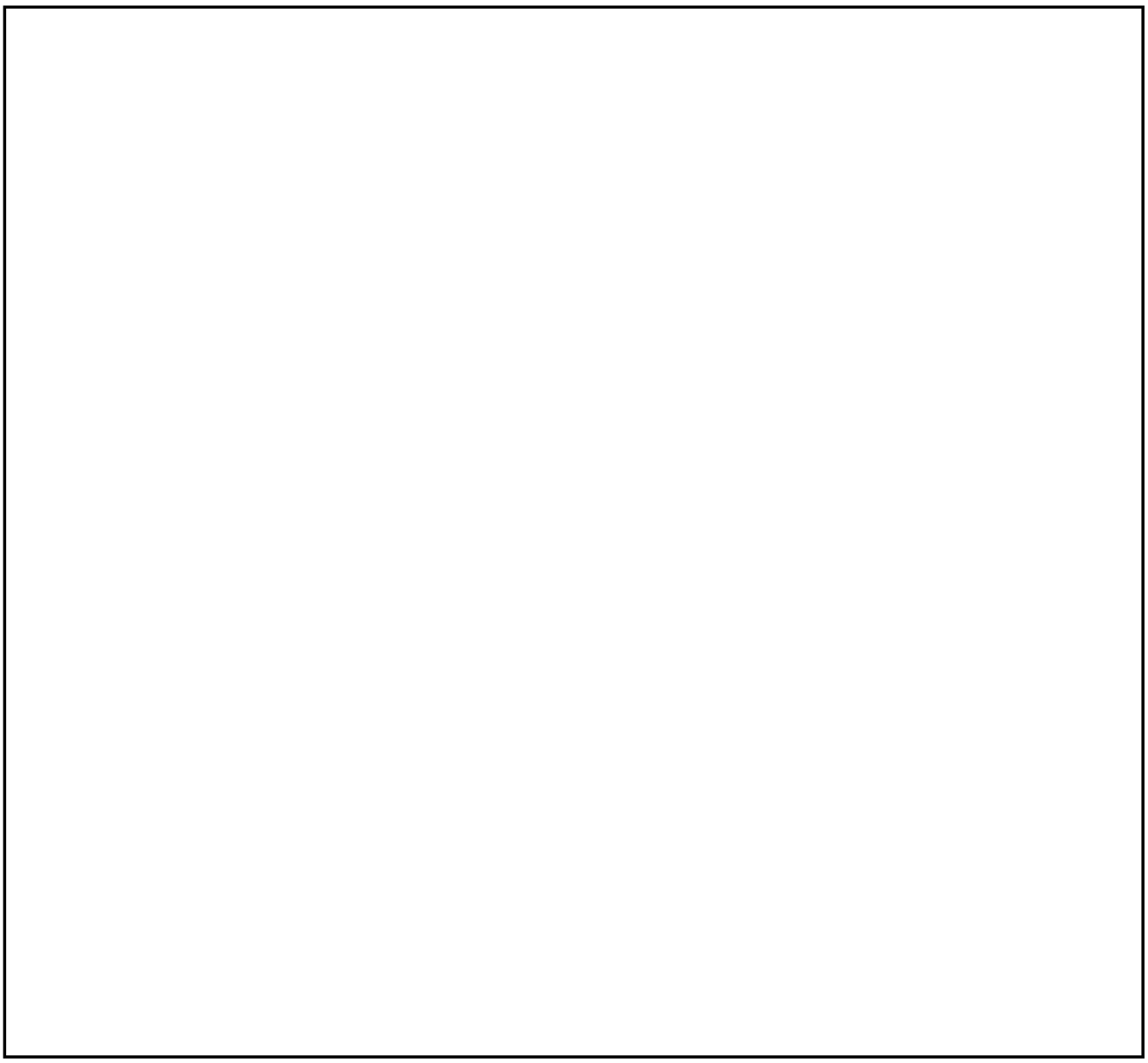
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



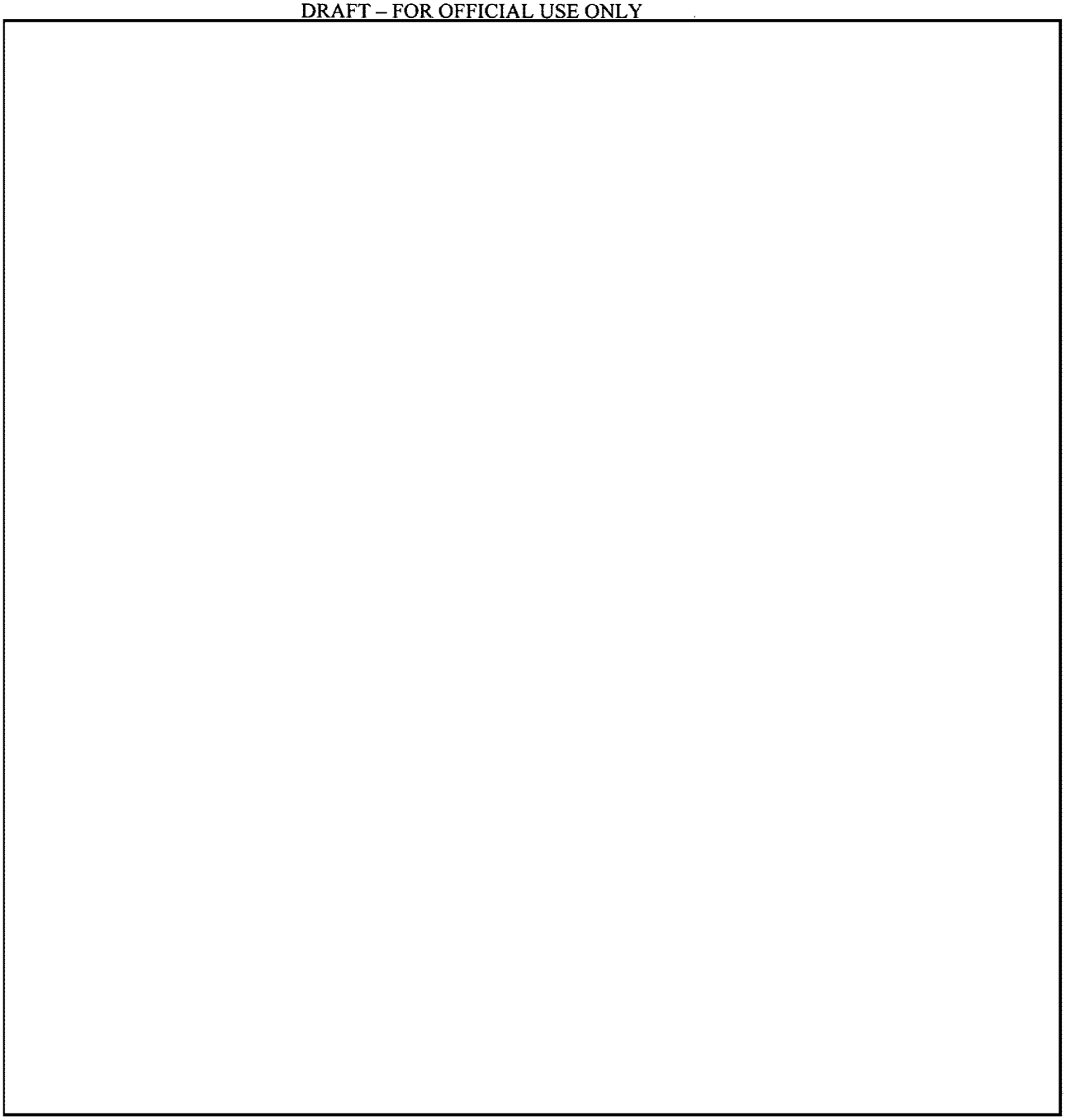
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



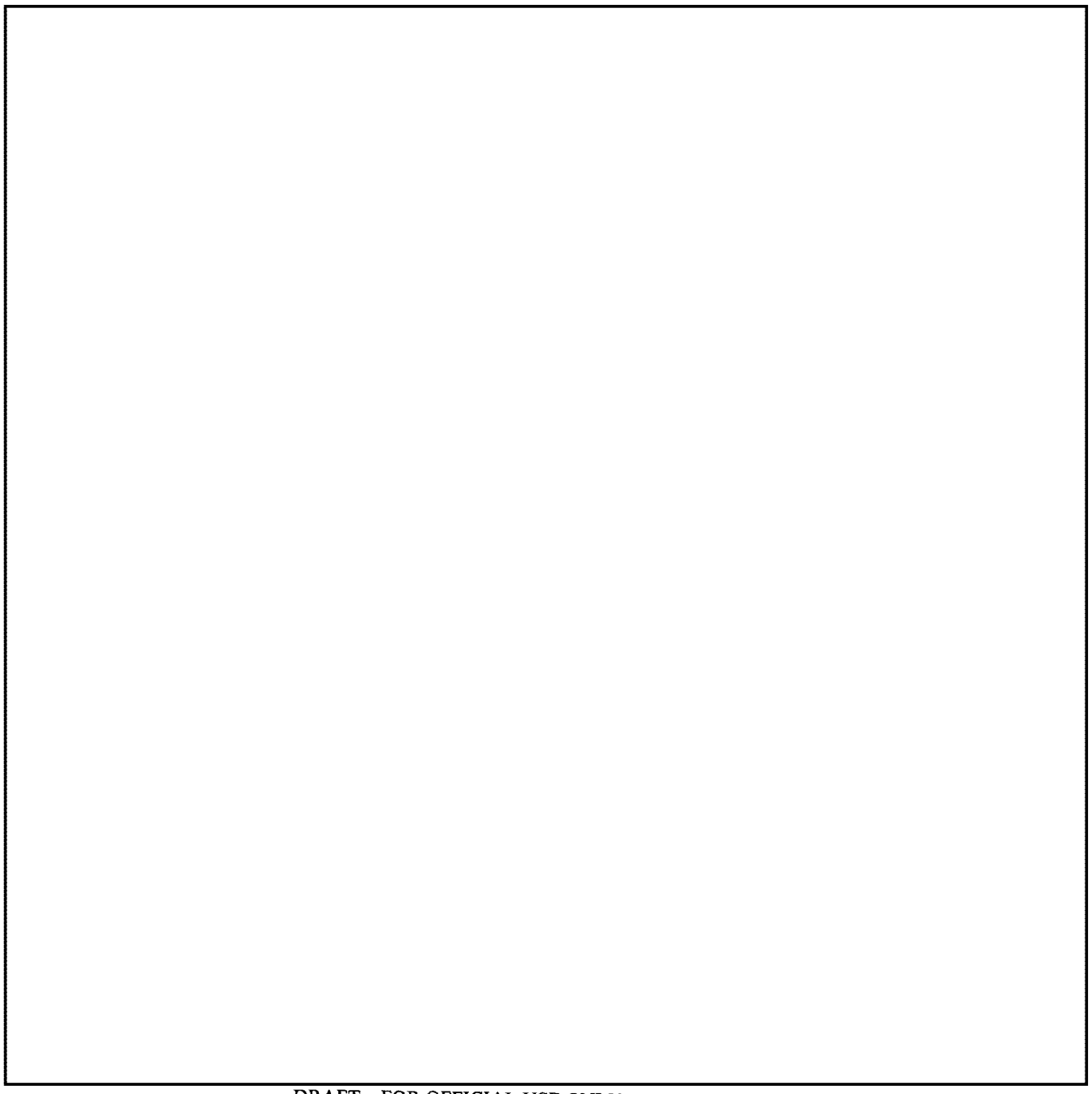
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



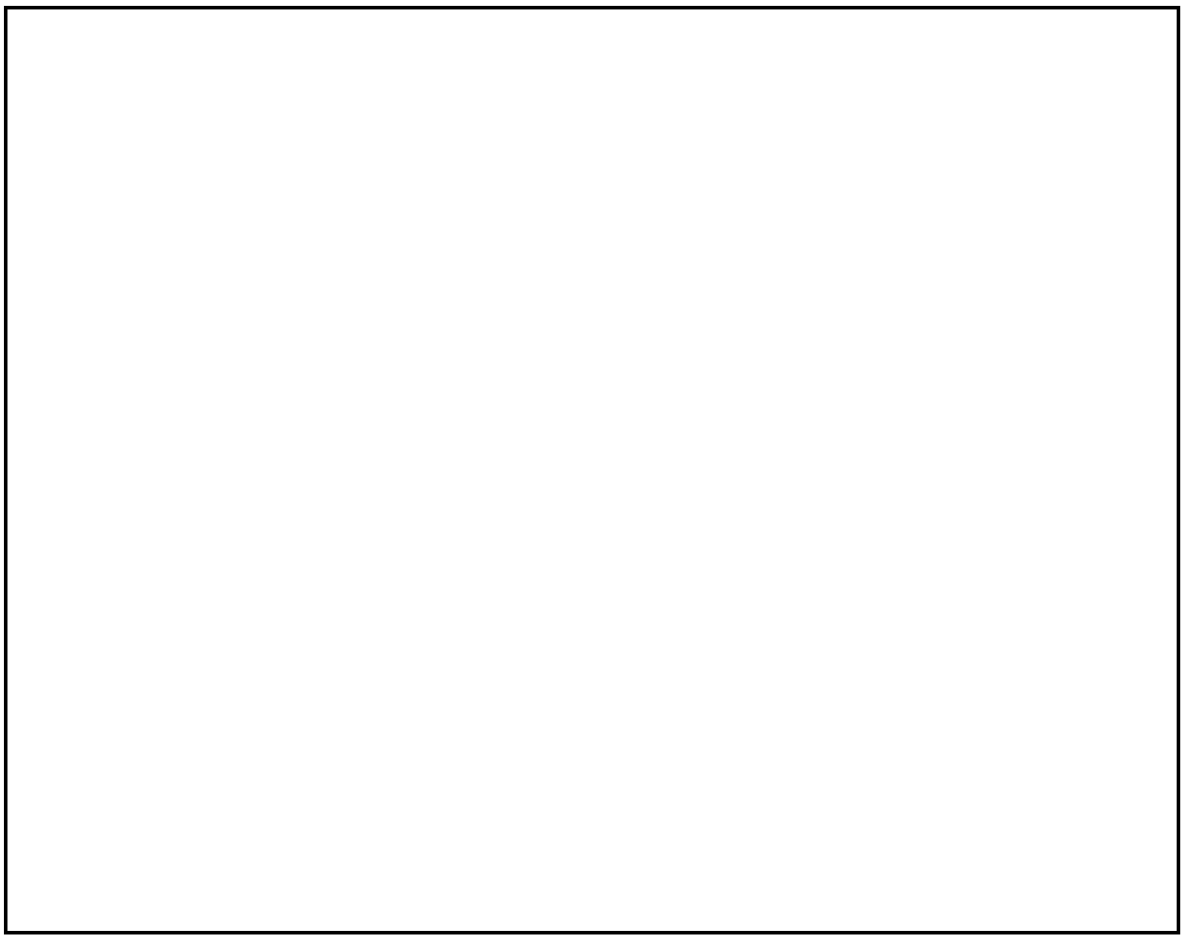
PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5



PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

[redacted] b5

[redacted] (S)

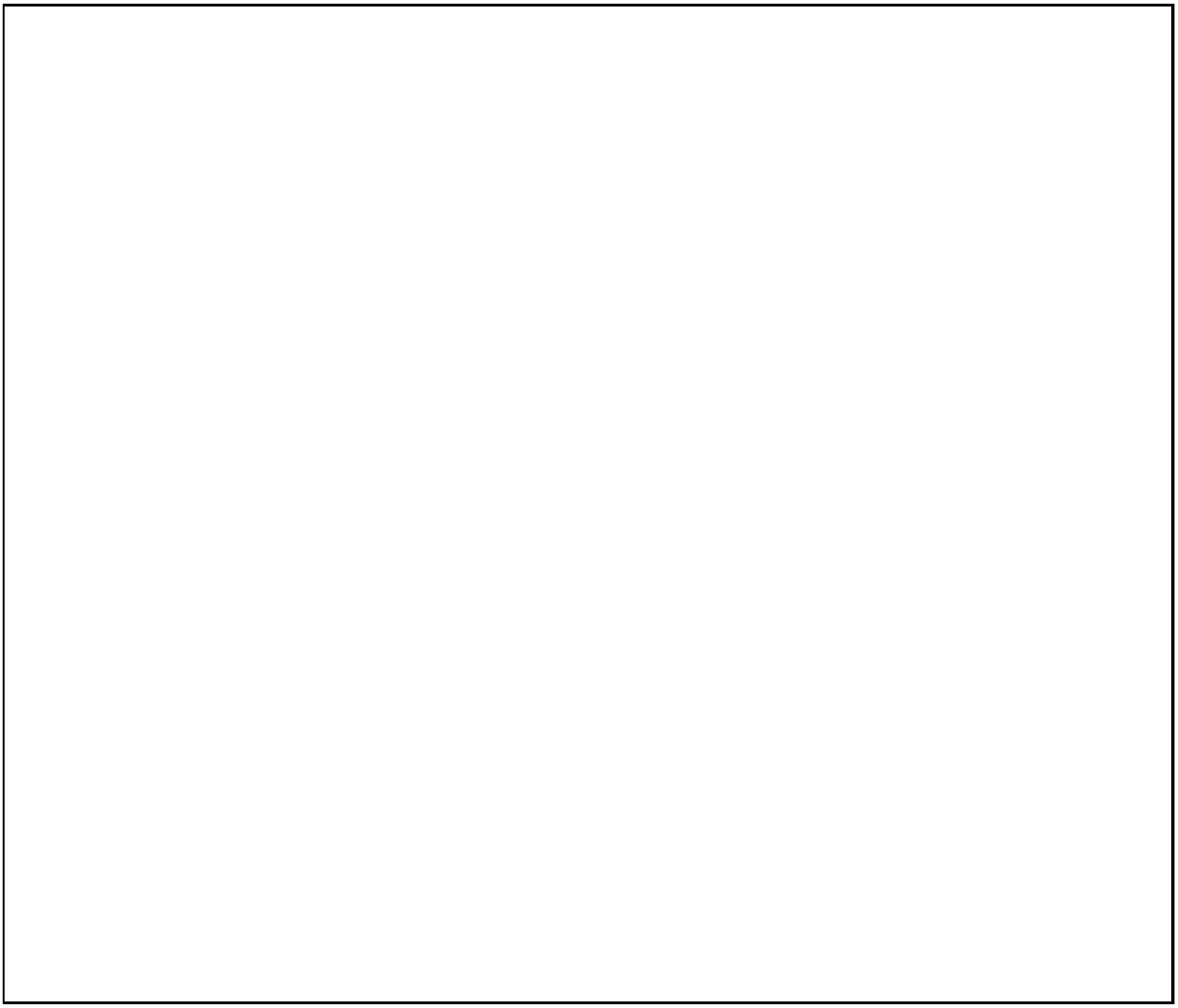
b5
b1

[redacted] (S)

b1
b5

[redacted] b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

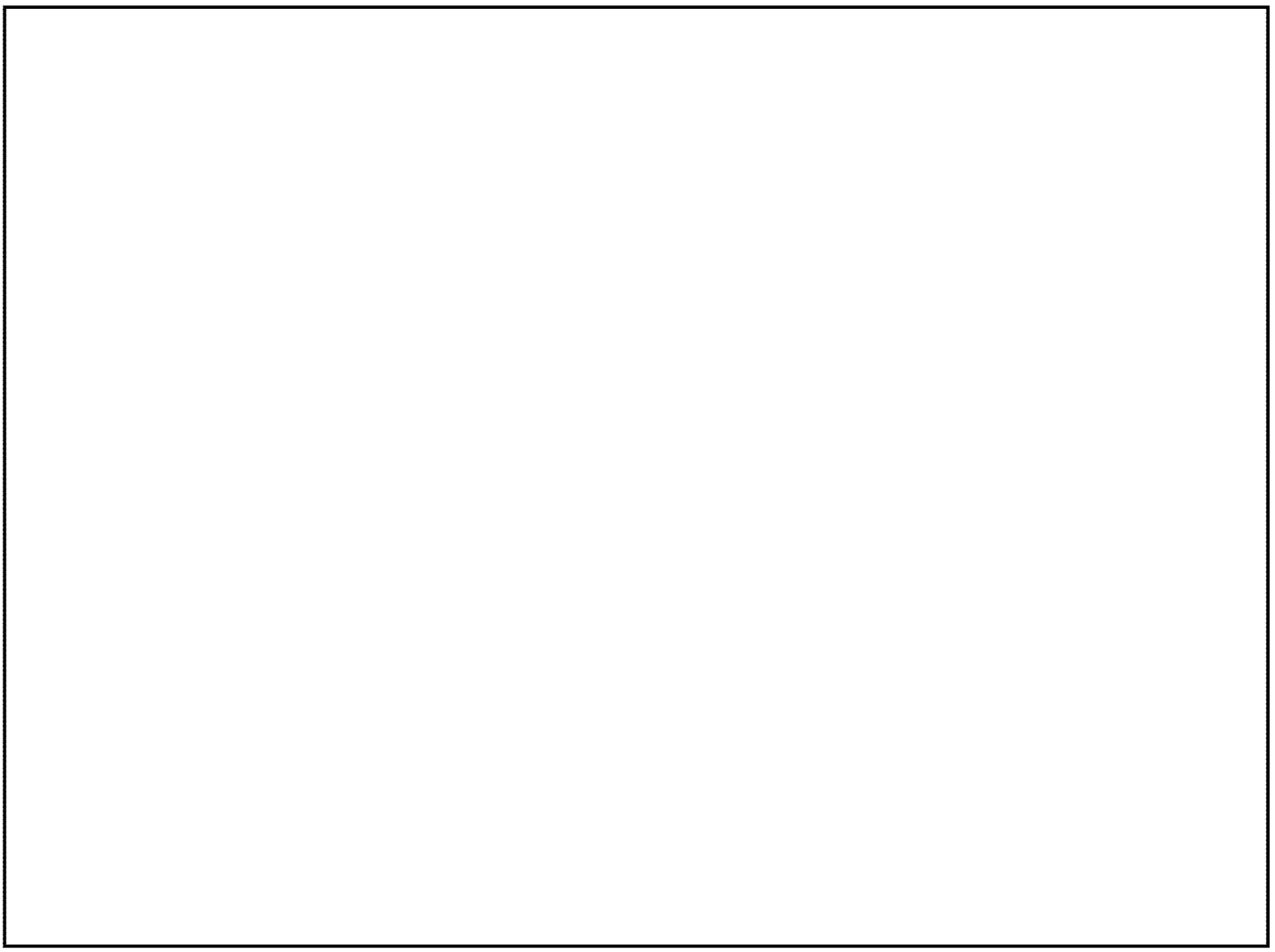


PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

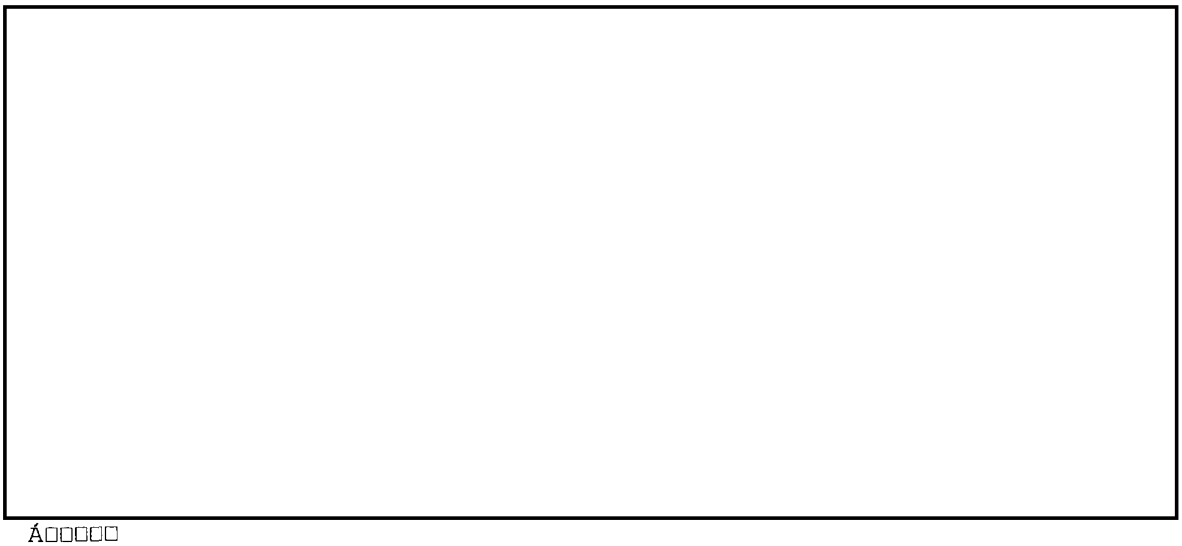
b5



ÄÁ□Ø Ø □□ÁTerrorist DNA database

b5
b6
b7C

Ð□Ð□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□°□□□`
□□h□À□□□p□È□ x Ð (#€%Ø'0*^,à.81▯3è5@8~:ð<H? AøCPF¨H□KXM°O□R`T V□Yh[À]
□`□□□□□□□□□□□□□□□□□□□□□□□□°□Ð□□ [redacted]



b5

Á□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□ÁÁ□□□□□
□Á
Á□□□□
□Áa.

b5

Á□□□□□
□Áb.

Á□□□□

b5

Á□□□□□
□Á2)

b5

Á□□□

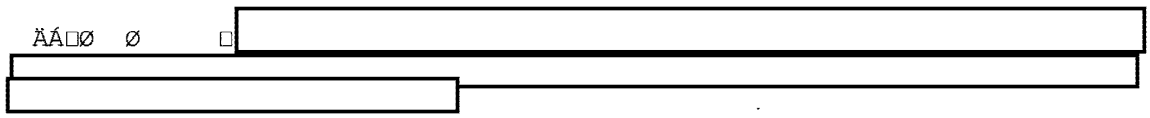
b5

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

b5
b6
b7C

Ð□Ð□□Ø ÿÿ□□□□□□□□□□□□□□□□□□□□□□□□□□□°□Ð□□Ð
Ã

ĀCC:Ä



b5
b6
b7C

Information Sharing Requirements

PATRIOT ACT

§ 203 ***Authority to share criminal investigative information***

(a) ***Authority to share grand jury information***

(1) Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure is amended by the following:

(C)(i) Disclosure of grand jury information may be made-

(V) when matters involve foreign and counter intelligence (as defined in the National Security Act) or foreign intelligence information (as defined in (iv)) to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

(iv) "Foreign intelligence" means -

(I) Information, whether or not concerning a United States person, that relates to the ability of the United States to protect against the following actions by a foreign power or agent of a foreign power: (aa) actual or potential attack or grave hostile acts; (bb) sabotage or international terrorism; (cc) clandestine intelligence activities by an intelligence service or network; or

(II) Information, whether or not concerning a United States person, with respect to a foreign power or a foreign territory that relates to (aa) the national defense or security of the United Sates; or (bb) the conduct of the foreign affairs of the United Sates.

(b) ***Authority to share electronic, wire, and oral interception information***

(6) Any law enforcement officer may disclose wire, oral, and electronic information, which includes foreign intelligence or counterintelligence information, to any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

(c) ***Procedures***

The AG shall establish procedures for the disclosure of grand jury and electronic, wire, and oral interception information that identifies a United States person as defined in FISA.

(d) ***Foreign Intelligence information***

(1) Notwithstanding any other provision of law, it shall be lawful to disclose information obtained as part of a criminal investigation.

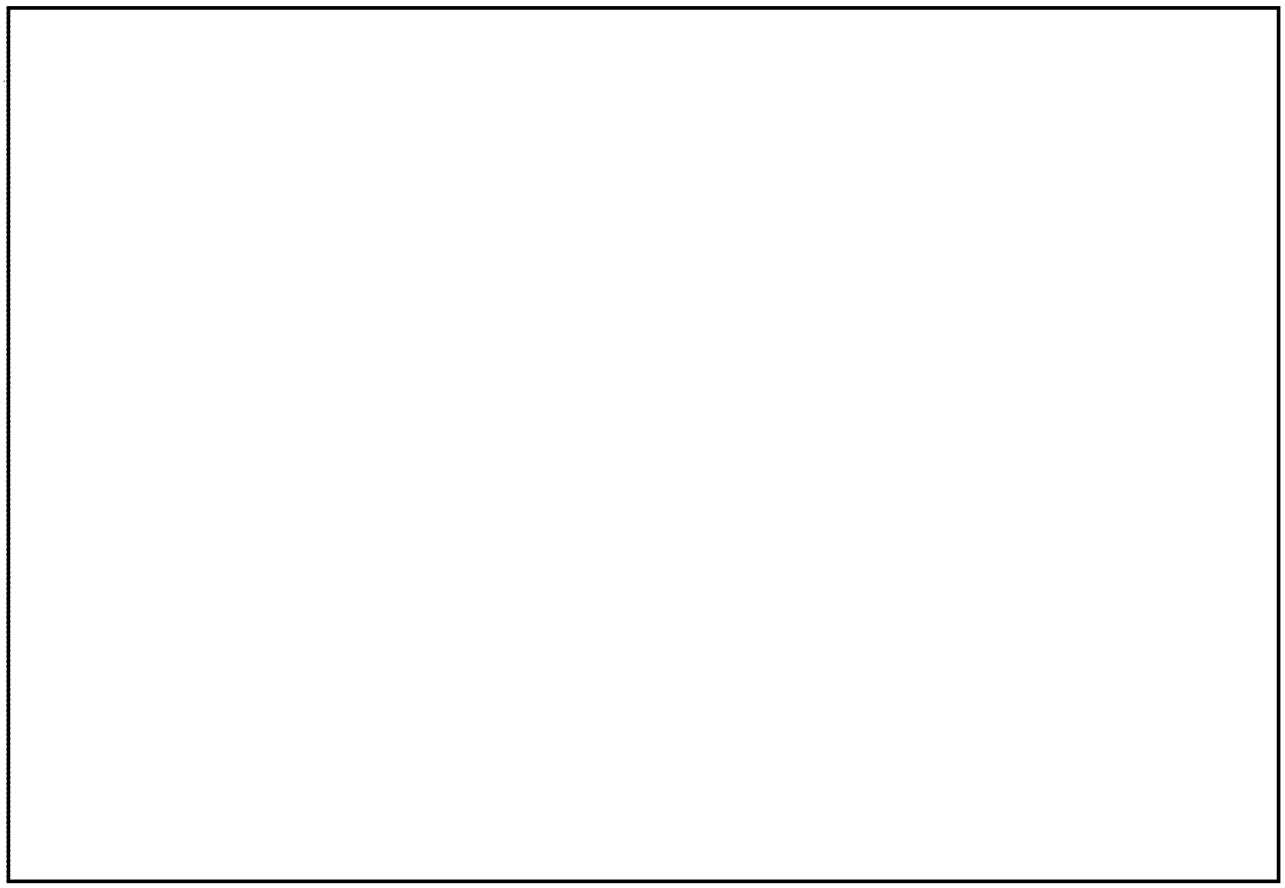
§ 905 ***Disclosure to the DCI of Foreign Intelligence-related information with respect to criminal investigations***

[§ 905 amends Title I of the National Security Act of 1947]

(a) Except as otherwise provided by law, the AG or head of any other department or agency with law enforcement responsibilities shall expeditiously disclose to the DCI foreign intelligence acquired in the course of a criminal investigation pursuant to guidelines developed by the AG and DCI. The AG and the DCI may provide for exceptions if disclosure would jeopardize an ongoing investigation or impair other significant law enforcement issues.

(b) The AG and DCI shall develop guidelines to ensure that after receipt of foreign intelligence activity, the AG provides notice to DCI of any intention to commence or decline to commence a criminal investigation.

(c) The AG shall develop procedures for the administration of this section.



HOMELAND SECURITY ACT
TITLE II – INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION
SUBTITLE A – DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION; ACCESS TO INFORMATION
§ 201 ***Directorate for Information Analysis and Infrastructure protection***
(d) ***Responsibilities of the Undersecretary***

The responsibilities of the Undersecretary for Information Analysis and Infrastructure Protection of the Department of Homeland Security ("DHS") shall be as follows:

(4) to ensure, pursuant to section 202, the timely and efficient access by the DHS to all information necessary to discharge the responsibilities under this section, including obtaining such information from other federal agencies.

(9) to disseminate, as appropriate, information analyzed by the DHS to other federal agencies with responsibilities relating to homeland security in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks.

(10) to consult with the DC I and other intelligence, law enforcement, or other agencies to establish collection priorities and strategies for information, including law enforcement-related information, relating to threats of terrorism.

(12) to ensure that

(A) any material received pursuant to this Act is protected from unauthorized disclosure.

(B) any intelligence information obtained is shared, retained, and disseminated consistent with the authority of the DCI to protect intelligence sources and methods under the

NSA of 1947 and, as appropriate, similar authorities of the AG concerning sensitive law enforcement information.

(13) to request additional information from federal agencies relating to threats of terrorism, including the entry into cooperative agreements through the Secretary of Homeland Security ("Secretary") to obtain such information.

(17) to coordinate with elements of the intelligence community and with federal, state, and local law enforcement agencies, as appropriate.

§ 202 ***Access to information***

(a) In general –

(1) ***Threat and vulnerability information***

Except as otherwise directed by the President, the Secretary shall have such access as the Secretary considers necessary to all information, that may be collected, possessed, or prepared by a federal agency, relating to threats of terrorism and concerning the infrastructure and vulnerabilities of the United States to terrorism and to other areas of responsibility assigned by the Secretary, whether or not such information has been analyzed.

(2) ***Other information***

The Secretary shall also have access to other information relating to matters under the responsibility of the Secretary that may be collected, possessed, or prepared by a federal agency as the President may further provide.

(b) ***Manner of access***

Except as otherwise directed by the President-

(1) The Secretary may obtain information upon request and may enter into cooperative agreements to provide the information to others or provide the DHS with access to it on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases; and

(2) Regardless of whether the Secretary has made any request or entered into any cooperative agreement, all federal agencies shall promptly provide the Secretary with the following information:

(A) all reports (include those not yet fully evaluated) relating to threats of terrorism and to other areas of responsibility of the Secretary.

(B) all information concerning the vulnerability of the infrastructure or other vulnerabilities of the United States to terrorism, whether or not such information has been analyzed.

(C) all other information relating to significant and credible threats of terrorism, whether or not such information has been analyzed.

(D) such other information or material as the President may direct.

(c) ***Treatment under certain laws***

The Secretary shall be deemed to be a federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be provided with all the information law enforcement is required to give to the DCI under any provision of the Patriot Act, Section 2517(6) of title 18 USC and Rule 6(e)(3)(C) of the Federal Rules of Criminal Procedure.

(d) ***Access to intelligence and other information***

(1) ***Access by elements of federal government-***

Nothing in this title shall preclude the intelligence community (as defined in the National Security Act of 1947) or any element of the Federal Government with responsibility for

analyzing or receiving any information.

(2) ***Sharing of information***

The Secretary, in consultation with the DCI, shall ensure that intelligence or terrorism-related information to which they have access is appropriately shared with elements of the Federal Government, as appropriate.

SUBTITLE B – CRITICAL INFRASTRUCTURE INFORMATION

§ 212 ***Definitions***

In this subtitle:

(1) "Agency" has the meaning given in 5 USC § 551.

(2) "Covered federal agency" means the DHS.

(3) "Critical Infrastructure Information" means nonpublic information relating to the security of critical infrastructure or protected systems -

(A) Interference with or attack on critical infrastructure or protected systems by either physical or computer-based attack that violates the law, harms interstate commerce, or threatens public health or safety.

(B) The ability of any critical infrastructure or protected system to resist such interference, including any planned or past assessment of the vulnerability of critical infrastructure or a protected system.

(C) Any planned or past operational problem or solution regarding critical infrastructure or protected systems.

(6) "Protected system"

(A) means any service, physical or computer-based system, process or procedure that directly or indirectly affects the viability of a facility or critical infrastructure; and

(B) includes any physical or computer-based system or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) "Voluntary" -

(A) In the case of submittal of critical infrastructure information to a covered federal agency, "voluntary" means the submittal thereof, without the agency compelling access or submission, that may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members. ("Information Sharing and Analysis Organization" defined in §212(5)).

(B) Exclusions to the definition of "voluntary" consist of actions brought under the securities laws and do not include information or statements regarding licensing or permitting determinations.

§ 214 ***Protection of voluntary shared critical infrastructure information***

(a) ***Protection***

(1) Notwithstanding any other provision of law, critical infrastructure information that is voluntarily submitted to a covered federal agency for use regarding security of critical infrastructure and protected systems when accompanied by an express statement specified in (2)-

(A) shall be exempt from disclosure under the Freedom of Information Act.

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official.

(D) shall not without written consent of the person or entity submitting such information be used or disclosed by any officer or employee of the United

States for purposes other than those of this subtitle, except: (i) in furtherance of a criminal investigation or prosecution; or (ii) to Congress or the Comptroller General.

(2) ***Express Statement***

"Express statement" means

(A) in the case of written information or records, a written marking indicating that the information is voluntarily submitted in expectation of protection from disclosure.

(B) in the case of oral information, a similar written statement submitted within a reasonable time following the oral communication.

(d) ***Treatment of voluntary submittal of information***

Voluntary submittal of information protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a federal agency under any other provision of law.

SUBTITLE C – INFORMATION SECURITY

§ 221 ***Procedures for sharing information***

The Secretary shall establish procedures on the use of information sharing under this title that

(3) protect the constitutional and statutory rights of any individuals who are subjects of such information.

TITLE VIII

SUBTITLE I – INFORMATION SHARING

§ 892 ***Facilitating homeland security information sharing procedures***

(a) ***Procedures for determining extent of sharing of homeland security information***

(1) The President shall prescribe and implement procedures applicable to all federal agencies for sharing homeland security information; identifying and safeguarding sensitive but unclassified homeland security information; and determining whether, how, and to what extent to remove classified information.

(b) ***Procedures for sharing of homeland security information***

(1) Under procedures prescribed by the President, homeland security information shall be shared to the extent such information can be shared and together with assessments of credibility.

(2) Each homeland security information sharing system shall (A) be able to transmit classified and unclassified information; (B) restrict delivery to specific recipients; (C) allow efficient and effective sharing; and (D) be accessible to state and local personnel.

(3) The procedures for sharing homeland security information shall establish conditions (A) to limit redissemination; (B) ensure security and confidentiality; (C) protect constitutional and statutory rights of individuals; and (D) provide data integrity through timely removal and destruction of obsolete and erroneous information.

(5) Each appropriate federal agency, as determined by the President, shall have access to the information described under paragraph (1).

(7) Under procedures developed by the DCI and the AG, each federal agency shall review and assess information gathered and shared by local and state agencies and integrate such information with existing intelligence.

(f) ***Definitions***

(1) "Homeland security information" means any information possessed by an agency that (A)

relates to the threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act.

(2) "Intelligence community" has the meaning given in § 401a(4) of the National Security Act of 1947.

§ 896 ***Authority to share electronic, wire, and oral interception information***

Amends 18 USC 2517.

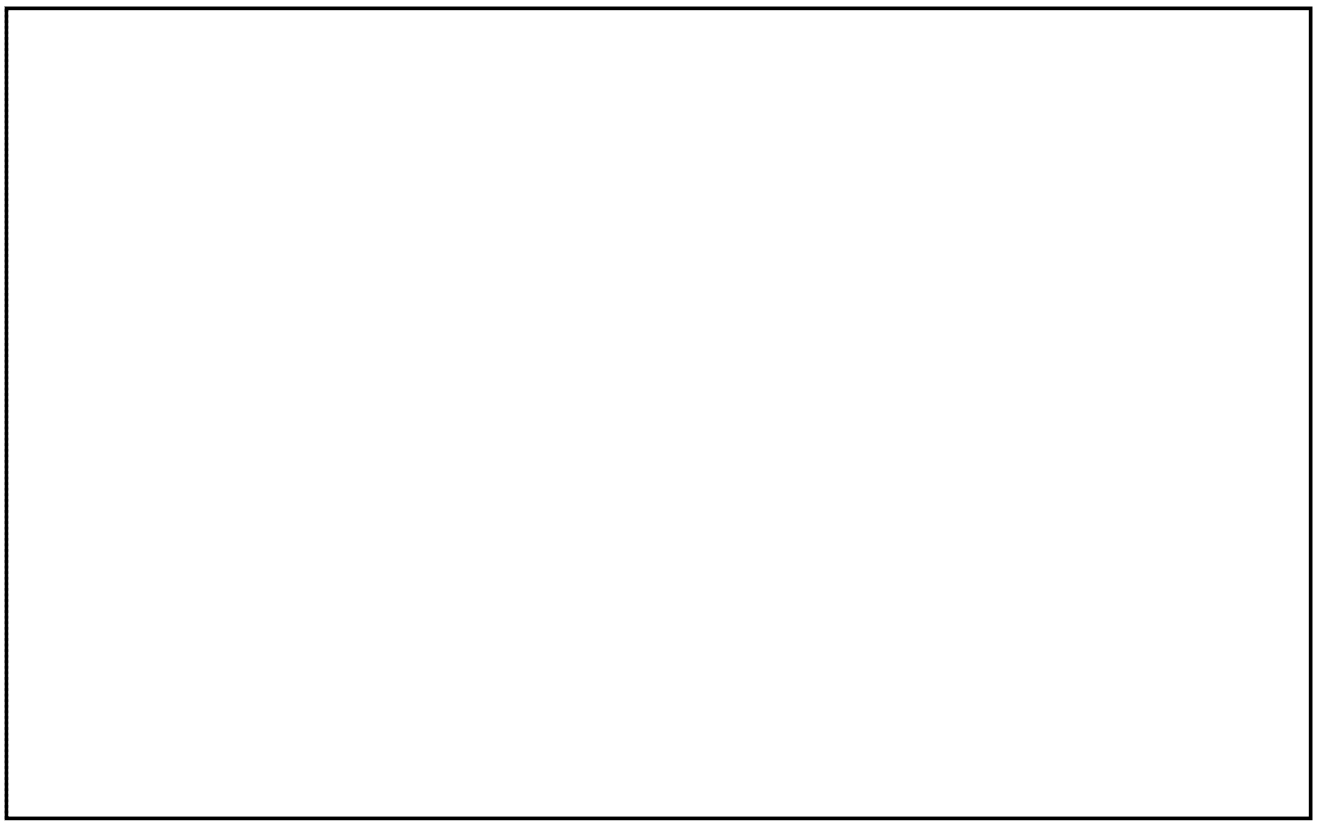
(7) Any investigative or law enforcement officer may disclose wire, oral, or electronic communication or evidence derived therefrom to a foreign investigative or law enforcement officer and vice versa.

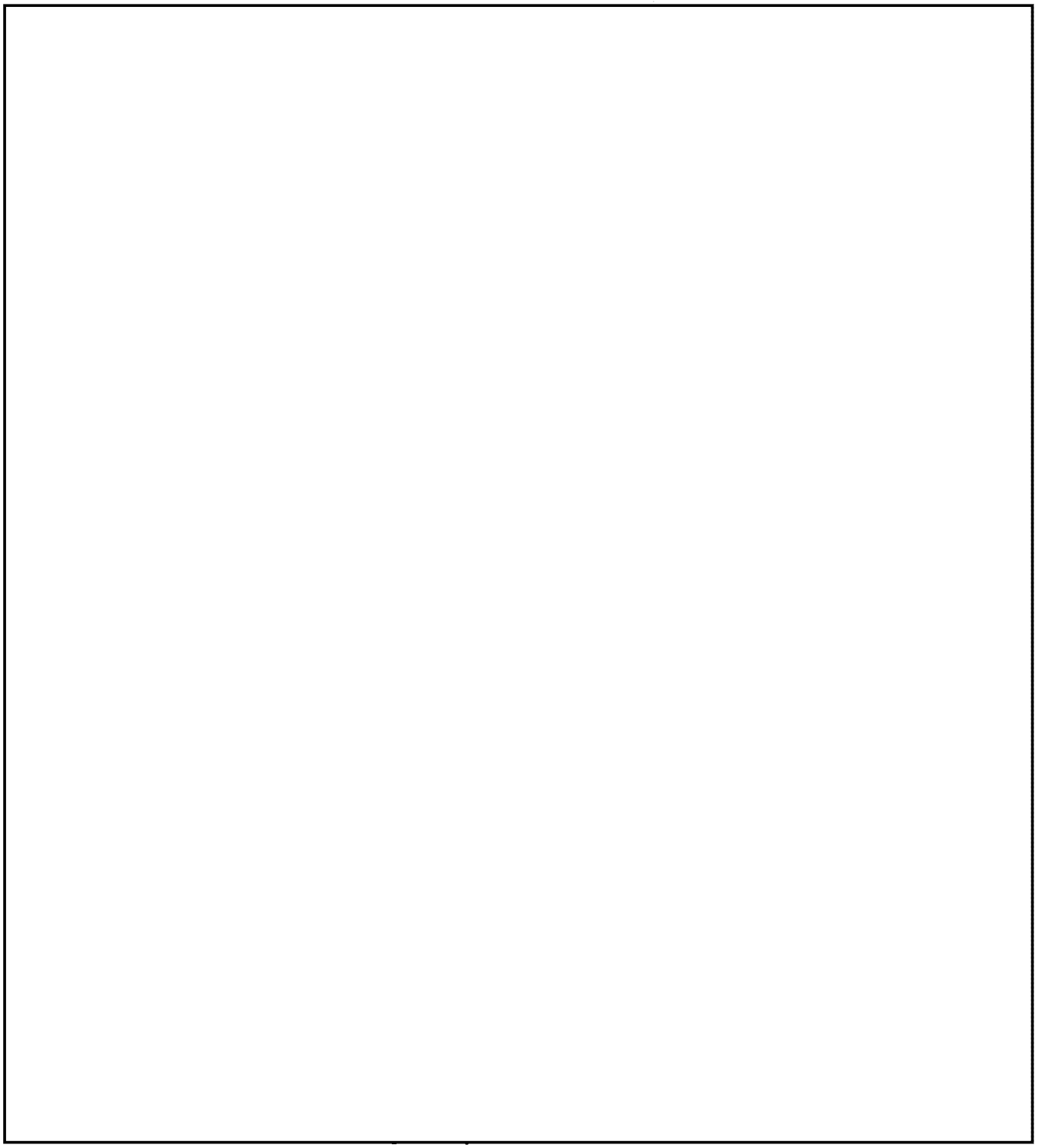
(8) Such information may be disclosed to any federal, state, local, or foreign government official when necessary to prevent or respond to threats of terrorist attacks, hostile acts, sabotage, or clandestine intelligence gathering activities by a foreign power or its agent ("threats of terrorism"). State, local, and foreign governments must follow guidelines issued by the AG and DCI.

§ 897 ***Foreign Intelligence Information***

(a) ***Dissemination authorized***

Amends Patriot Act section 203(d). It shall be lawful to disclose information revealing threats of terrorism obtained as part of a criminal investigation to appropriate federal, state, local, and foreign government officials for the purpose of preventing or responding to such threats. State, local, and foreign governments must follow guidelines issued by the AG and DCI.





NATIONAL SECURITY ACT OF 1947
§ 401a ***Definitions***
(1) "Intelligence" includes foreign intelligence and counterintelligence.

(2) "Foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(3) "Counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations, conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

(4) "National intelligence" and "intelligence related to the national security"-

A) each refer to intelligence which pertains to the interests of more than one department or agency of the Government; and

(B) do not refer to counterintelligence or law enforcement activities conducted by the FBI except to the extent provided for in procedures agreed to by the DCI and AG, or otherwise as expressly provided for in this title.

[See also §§ 403-5a(c), 403-5d(2)]

§ 402a ***Coordination of counterintelligence activities***

(e) ***Coordination of counterintelligence matters with the FBI***

(1) Except as provided in paragraph (5), the head of each department or agency of the executive branch shall ensure that-

(A) the FBI is advised immediately if classified information is or was disclosed in an unauthorized manner to a foreign power or agent.

(B) the FBI is consulted with respect to all subsequent actions which may be undertaken by the department or agency to determine the source of such loss or compromise, and

(C) Where the FBI undertakes investigative activities, the FBI is given complete and timely access to the department or agency's employees and records.

(2) Except as provided in paragraph (5), The Director of FBI shall ensure that espionage information pertaining to departments or agencies is provided to them in a timely manner and that they are consulted in a timely matter with respect to espionage investigations that concern them.

(3)

(A) The Director of FBI shall submit to the department or agency a written assessment of the potential impact of their actions on counterintelligence investigations.

(B) The department or agency shall evaluate the assessment to determine whether the subject of the investigation should be left in place and notify the FBI of such determination.

(C) The department or agency and the FBI shall continue to consult, review the status of the investigation, and reassess.

(5) When extraordinary circumstances affect national security, the President may on a case-by-case basis waive the requirements above.

§ 403-3 ***Responsibilities of the DCI***

(c) ***Head of the intelligence community***

(6) The DCI shall establish requirements for the collection of FI under FISA and provide assistance to the AG in disseminating information from electronic surveillance and physical searches under FISA. Except as otherwise authorized by statute or executive order, the DCI has no authority to direct, manage, or undertake electronic surveillances or physical searches pursuant to FISA.

(d) ***Head of the CIA***

(3) The DCI shall correlate, evaluate, and provide appropriate dissemination of intelligence related to national security.

§ 403-4 ***Authorities of the DCI***

(a) *Access to intelligence*

The DCI shall have access to all intelligence related to national security that is collected by any department, agency, or other entity of the United States (to the extent recommended by the NSC and the President).

§ 403-5a ***Assistance to United States law enforcement agencies***

(a) ***Authority to provide assistance***

Elements of the intelligence community may, upon request of United States law enforcement agencies, collect information outside the United States about individuals who are not United States persons, notwithstanding the intention of law enforcement agencies to use such information for law enforcement or counterintelligence investigations. (This is subject to limitations imposed by the DoD).

(c) ***Definitions***

(1) "United States law enforcement agency" means any department or agency of the Federal government that the AG designates as a law enforcement agency for the purposes of this section.

(2) "United States Person" means

(A) US citizen

(B) permanent alien resident

(C) unincorporated association composed of citizens or resident aliens

(D) corporation incorporated in the US (except for those directed or controlled by foreign governments).

§ 403-5b ***Disclosure of foreign intelligence acquired in criminal investigations; notice of criminal investigations of foreign intelligence sources***

(a) ***Disclosure of foreign intelligence***

(1) Except as otherwise provided by law, the AG or other law enforcement head shall expeditiously disclose to DCI, pursuant to guidelines developed by AG, FI acquired by the DOJ in the course of a criminal investigation.

(2) The AG can provide for exceptions if the AG determines that disclosure would jeopardize an ongoing law enforcement investigation or impair other significant law enforcement interests.

(b) ***Procedures for notice of criminal investigations***

The AG and DCI will develop guidelines to ensure that, after receipt of a report from the intelligence community about FI warranting a criminal investigation, the AG provides notice to the DCI within a reasonable period of time of any intention to commence or decline to commence a criminal investigation.

(c) *Procedures*

The AG shall develop procedures for the administration of this section.

§ 403-5d ***Foreign Intelligence information***

(1) ***In general***

Notwithstanding any other provision of law, it shall be lawful for FI obtained as part of a criminal investigation to be disclosed to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official.

(2) ***Definitions***

"Foreign intelligence" means

(A) information, whether or not concerning a United States person, that relates to protection against the following actions by a foreign government or its agents: (i) actual or potential attacks or hostile acts; (ii) sabotage or international terrorism; (iii) clandestine intelligence activities.

(B) information, whether or not concerning a United States person, with respect to a foreign power or agent that relates to: (i) national defense or security; (ii) conduct of the foreign affairs of the United States.

EO 12333

Part 1

Goals, Direction, Duties and Responsibilities with respect to the National Intelligence Effort

1.1 ***Goals***

The United States intelligence effort shall provide the President and National Security Council with necessary information on which to base the conduct and development of foreign, defense, and economic policy, and the protection of the United States national interests from foreign security threats. All departments and agencies shall cooperate fully.

(a) Maximum emphasis should focus on analytical competition among the intelligence community.

(b) All means, consistent with United States law and this Order, and with full consideration of the rights of US persons, shall be used to develop intelligence.

(d) To the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of US persons, all agencies shall ensure full and free exchange of information.

1.4 ***The Intelligence Community***

In accordance with applicable US law and with the other provisions of this Order, agencies within the Intelligence Community shall:

(a) Collect information needed by the President, the National Security Council, the Secretaries and State and Defense, and other Executive Branch officials.

(b) Protect and disseminate intelligence.

(c) Collect information concerning intelligence activities directed against the United States and concerning activities to protect against such conduct.

1.5 ***Director of Central Intelligence***

The DCI shall be responsible directly to the President and the NSC and shall:

(a) Act as their primary advisor on foreign national intelligence and provide them and other officials within the Executive Branch with national foreign intelligence.

(i) Establish uniform criteria for determining relative priorities for the transmission of critical national foreign intelligence.

(k) Have full responsibility for producing and disseminating national foreign intelligence. Have authority to levy analytic tasks on departmental intelligence production organizations, ensuring that competitive analysis, diverse points of view, and differences of judgment are brought to the attention of national policy makers.

(l) Ensure the timely exploitation and dissemination of foreign intelligence including dissemination to appropriate government entities and military commands.

(m) In accordance with the law and relevant procedures approved by the AG under this Order, give departments and agencies access to all intelligence relevant to their national intelligence

needs.

1.6 ***Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies***

(a) In accordance with the law and AG procedures under this Order, the heads of all executive branch departments and agencies shall give the DCI access to all information relevant to the national intelligence needs of the United States.

1.7 ***Senior Officials of the Intelligence Community***

The heads of departments or agencies within the IC shall:

(f) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the DCI.

1.8 ***The Central Intelligence Agency***

As authorized by this Order, the National Security Act of 1947, the CIA Act of 1949, and appropriate directives or other applicable law, the CIA shall:

(a) Collect, produce, and disseminate foreign intelligence and counterintelligence, including information not otherwise obtainable, in coordination with the FBI under procedures of the AG and DCI.

(b) Collect, produce, and disseminate intelligence on foreign aspects of narcotics production and trafficking.

1.14 ***The FBI***

Pursuant to regulations established by the AG, the Director of the FBI shall:

(d) Produce and disseminate foreign intelligence and counterintelligence.

Part 2

Conduct of Intelligence Activities

2.3 ***Collection of Information***

Agencies within the IC are authorized to collect, retain, or disseminate the following information concerning US persons in accordance with procedures developed by the heads of the agencies and approved by the AG:

(a) Information that is publicly available or collected with the consent of the person concerned.

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations.

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics, or international terrorism investigation.

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations.

(e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure.

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility.

(g) Information arising out of a lawful personnel, physical, or communications security investigation.

(h) Information acquired by overhead reconnaissance not directed at specific US persons.

(i) I ncidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws.

(j) I nformation necessary for administrative purposes.

Agencies within the IC can disseminate this information to each other.

2.4 ***Collection Techniques***

The IC cannot use the following collection techniques regarding US persons: electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency and approved by the AG. Such procedures shall protect constitutional and other legal rights, use the least intrusive means possible, and limit the use of such information to lawful governmental purposes.

3.4 *Definitions*

(a) "Counterintelligence" means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communication security programs.

(d) "Foreign intelligence" means information relating to the capabilities, intentions, and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities.

(e) "Intelligence activities" means all activities that agencies within the IC are authorized to conduct pursuant to this Order.

(f) "US Person" means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporation in the United States, except for a corporation directed and controlled by a foreign government or governments.

From [redacted] (OGC) (FBI)
Sent: Friday, October 22, 2004 7:44 PM
To: [redacted] OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From [redacted] (OGC) (FBI)
Sent: Friday, October 22, 2004 10:15 AM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (CTD) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C

b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

PRIVILEGED AND CONFIDENTIAL
ATTORNEY WORK PRODUCT

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, October 22, 2004 9:44 AM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (CTD) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C
b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, October 21, 2004 12:20 PM
To: [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: INTEL POLICY MANUAL

b6
b7C
b5
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, October 19, 2004 8:21 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI)
Subject: INTEL POLICY MANUAL

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Attached is what we hope is the final draft of the Intel Policy Manual you previously reviewed. We have taken into account all of your concerns as best we could, with the possible exception of [redacted] question about subjecting disseminations to the White House to the NSIG. Y'all take a closer look at that issue, in particular, and you don't like it, we can discuss it. I intend to make a side-by-side comparion of an AG memo [redacted] gave me last week with the info-sharing provisions of the NSIG. Absent some epiphany, however, this is how we intend to proceed, unless Valerie tells Maureen it's legally objectionable.

b6
b7C

FYI, in addition to concerns y'all raised specifically, [redacted] and I went back thru the whole thing with the *spirit* of your concerns in mind and rewrote some things y'all did not address. We think the result is a much better product than we had before. OI started this project with intent of producing a 70% solution quickly, then supplementing it as time and experience goes by. That didn't happen. As it turns out, however, I think what's attached in better than 70%, due in no small measure to your participation. So, thanks.

I hate to say we're rushed, but we need to report to the DOJ/IG by the end of the week (or maybe early next week) as to the status of this manual, so I need your comments ASAP.

Homer

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 42
Page 5 ~ Duplicate
Page 6 ~ Duplicate
Page 7 ~ Duplicate
Page 8 ~ Duplicate
Page 9 ~ Duplicate
Page 10 ~ Duplicate
Page 11 ~ Duplicate
Page 12 ~ Duplicate
Page 13 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 16 ~ Duplicate
Page 17 ~ Duplicate
Page 18 ~ Duplicate
Page 19 ~ Duplicate
Page 21 ~ Referral/Direct
Page 24 ~ Referral/Direct
Page 25 ~ Referral/Direct
Page 31 ~ Referral/Direct
Page 32 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 139 ~ Duplicate
Page 140 ~ Duplicate
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Duplicate
Page 145 ~ Duplicate
Page 309 ~ Duplicate
Page 324 ~ Duplicate
Page 325 ~ Duplicate
Page 326 ~ Duplicate
Page 328 ~ Referral/Direct
Page 329 ~ Referral/Direct
Page 335 ~ Referral/Direct
Page 336 ~ Referral/Direct
Page 337 ~ Referral/Direct
Page 338 ~ Referral/Direct
Page 339 ~ Referral/Direct

O/S

OFFICE OF

CONGRESSIONAL AFFAIRS

(Documents in response to EPIC's FOIA Lawsuit)

[redacted] (OCA) (FBI) b6 b7C

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website (http://oca.fbinet.fbi) under the "Legislation of Interest" link.

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

Patriot Act Sunset Provisions

Section	Description	Comment
201	These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), and terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B).	
202	These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to felony violations of computer fraud and abuse (18 U.S.C. § 1030).	
203(b)	Authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. (Wiretap info)	
203(d)	Authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. ("Catch-all" / non-wiretap or 6(e))	
204	Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications	

b5

Section	Description	Comment
206	Roving FISA Surveillance	
207	Extended Duration for Certain FISAs	
209	Seizure of Voice Mail with a Search Warrant	

b5

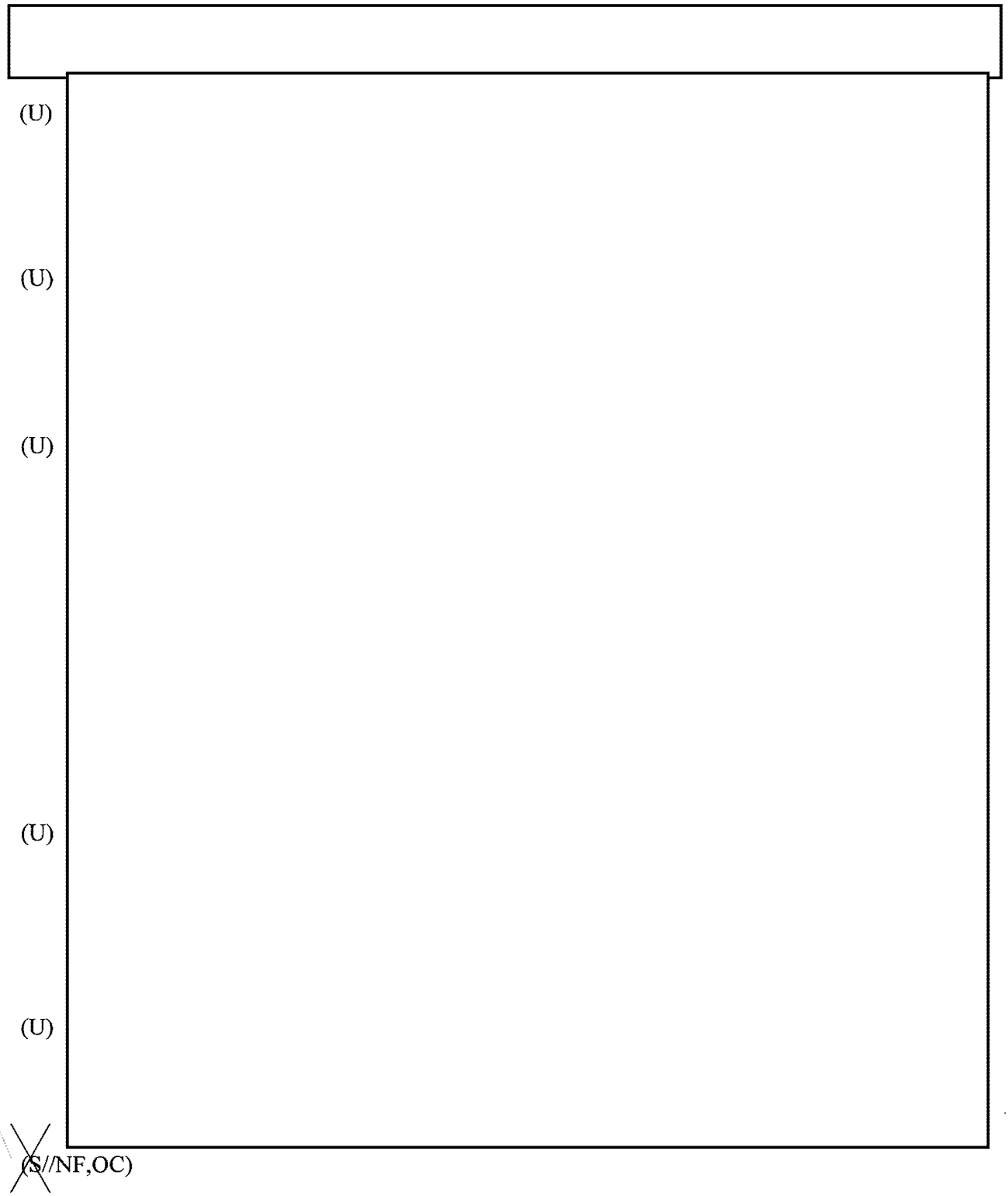
Section	Description	Comment
212	Emergency Disclosures of E-mail & Records by ISPs	
214	FISA Pen/Trap Authority	
215	Access to Business Records under FISA	
217	Interception of Computer Trespasser Communications	

b5

Section	Description	Comment
218	Change in the "Primary Purpose" Standard of FISA	
220	Nationwide Search Warrants for Electronic Evidence	
223	Civil Liability for Certain Unauthorized Disclosures	
225	Immunity for Compliance with FISA Wiretap	

b5

b5



(U)

(U)

(U)

(U)

(U)

(U)

(S//NF,OC)

(U)

(U)

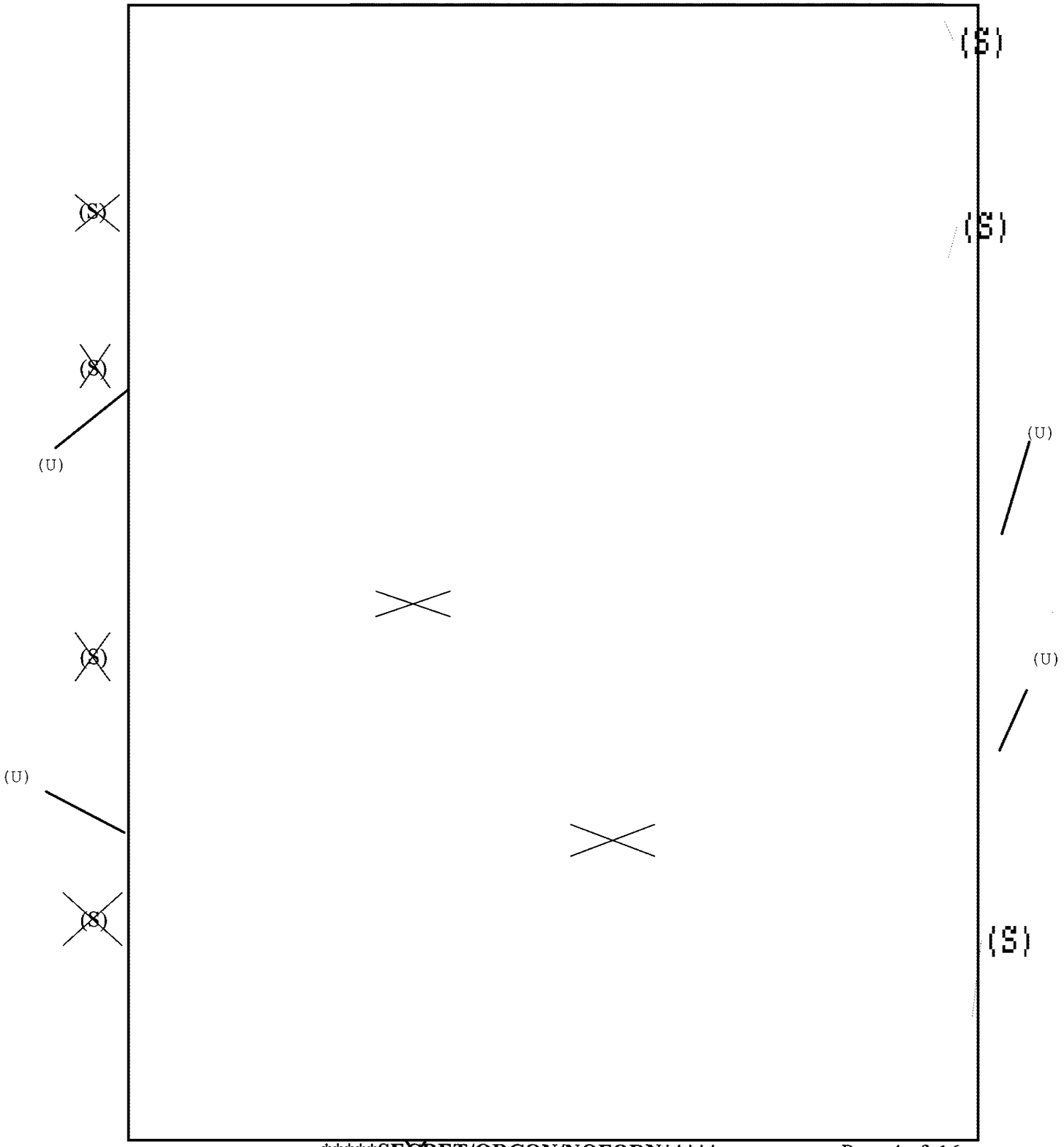
(S) (U)

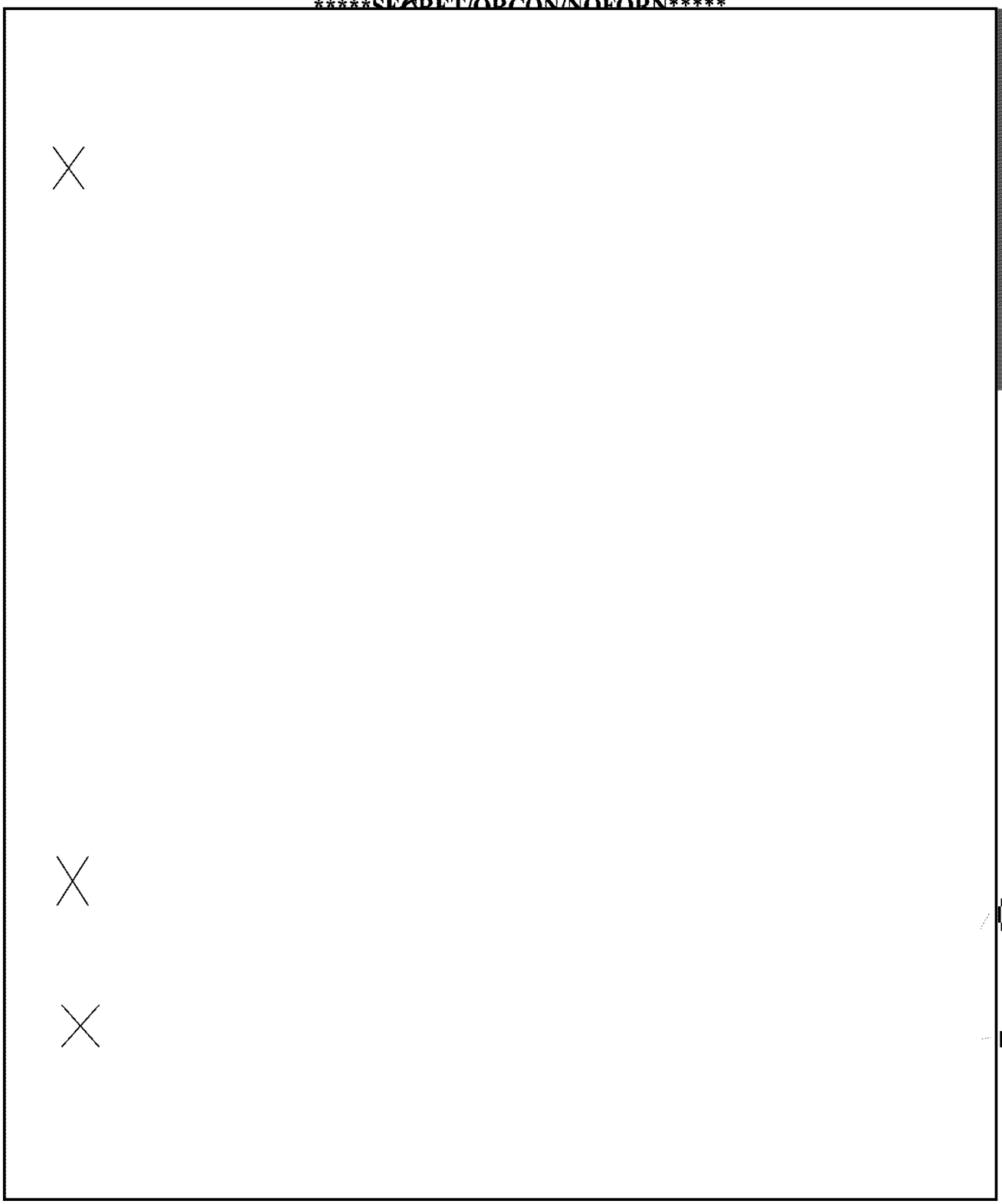
(S)

(S)

(S)

b1
b5
b6
b7A
b7C

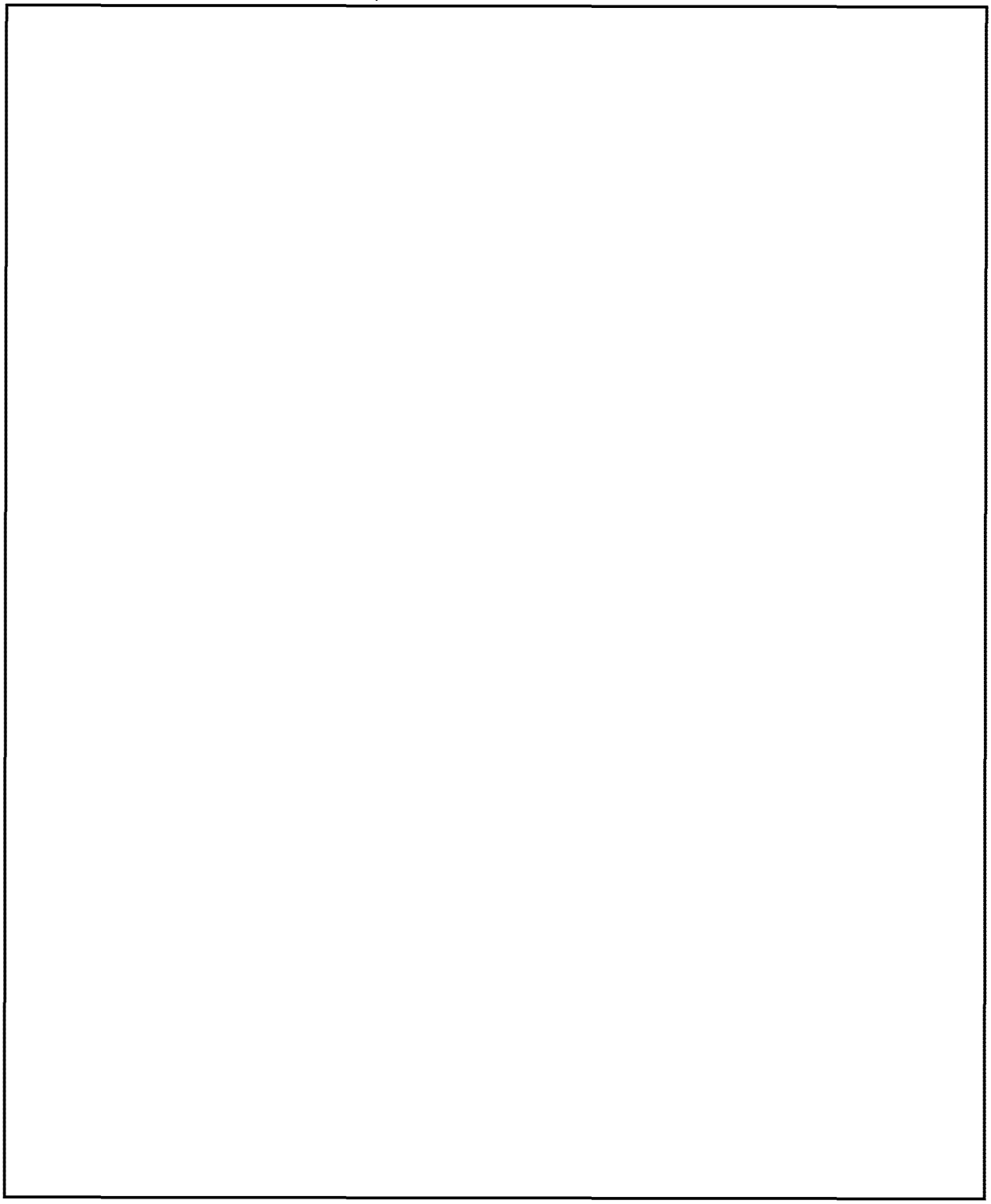


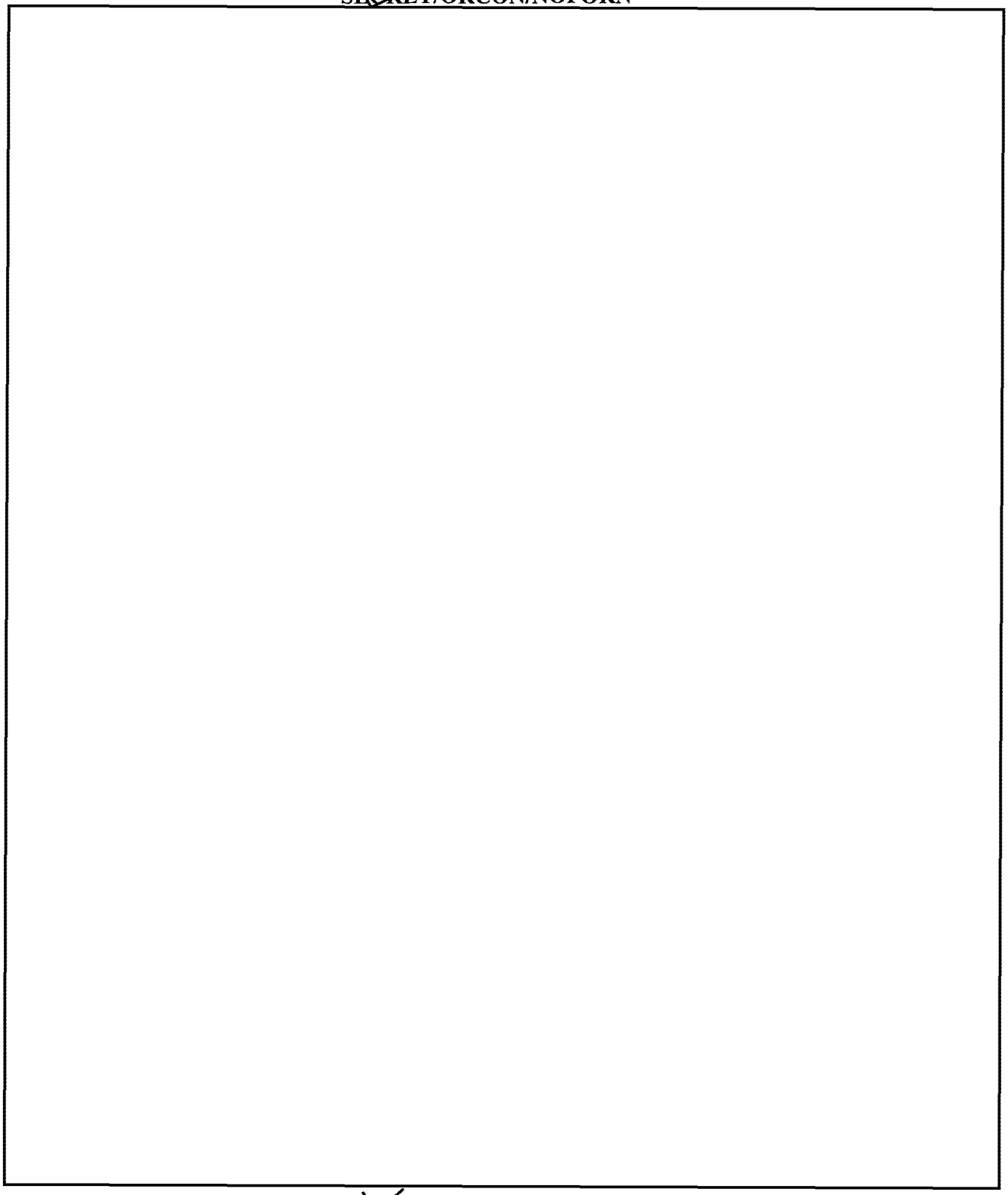


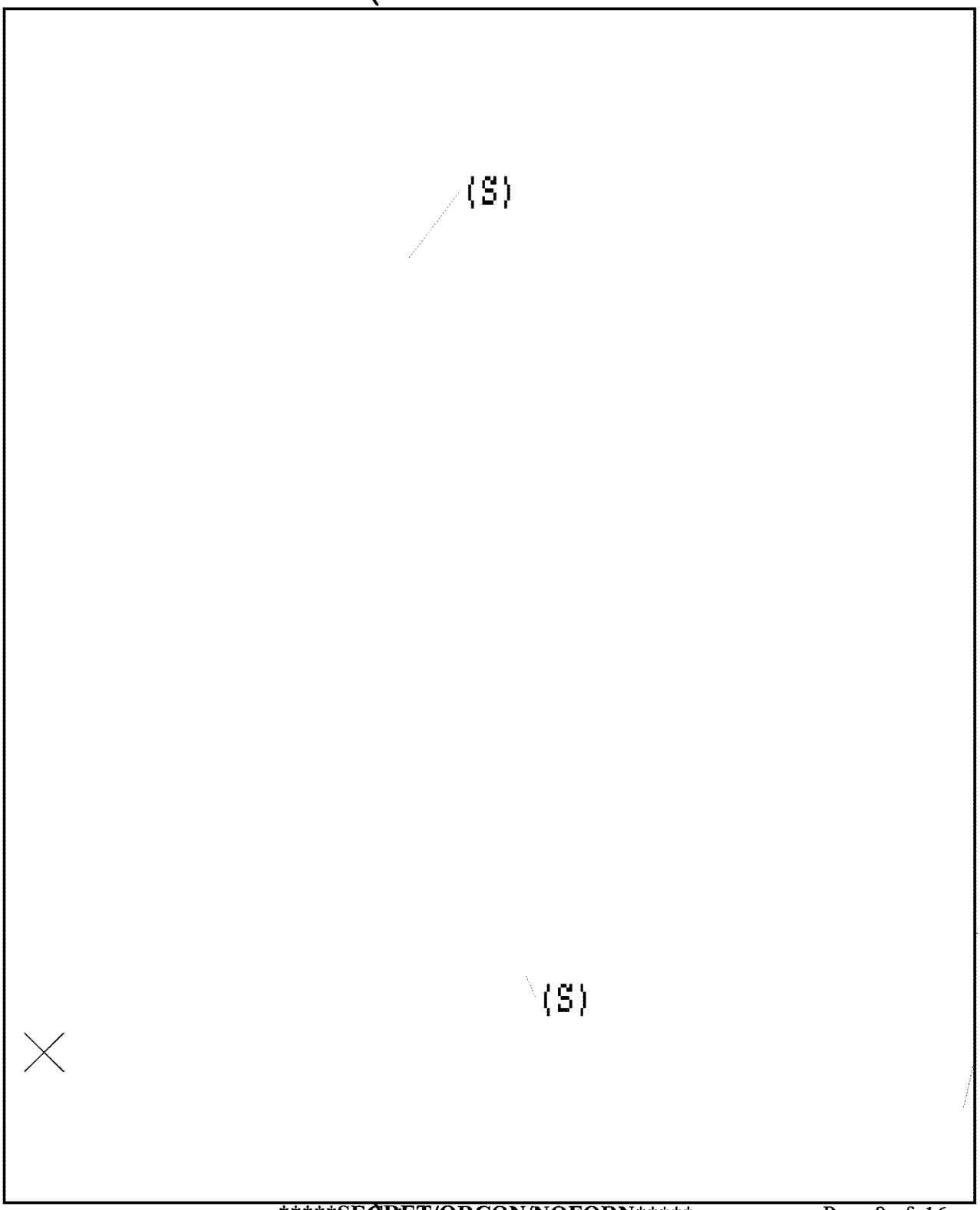
(S)

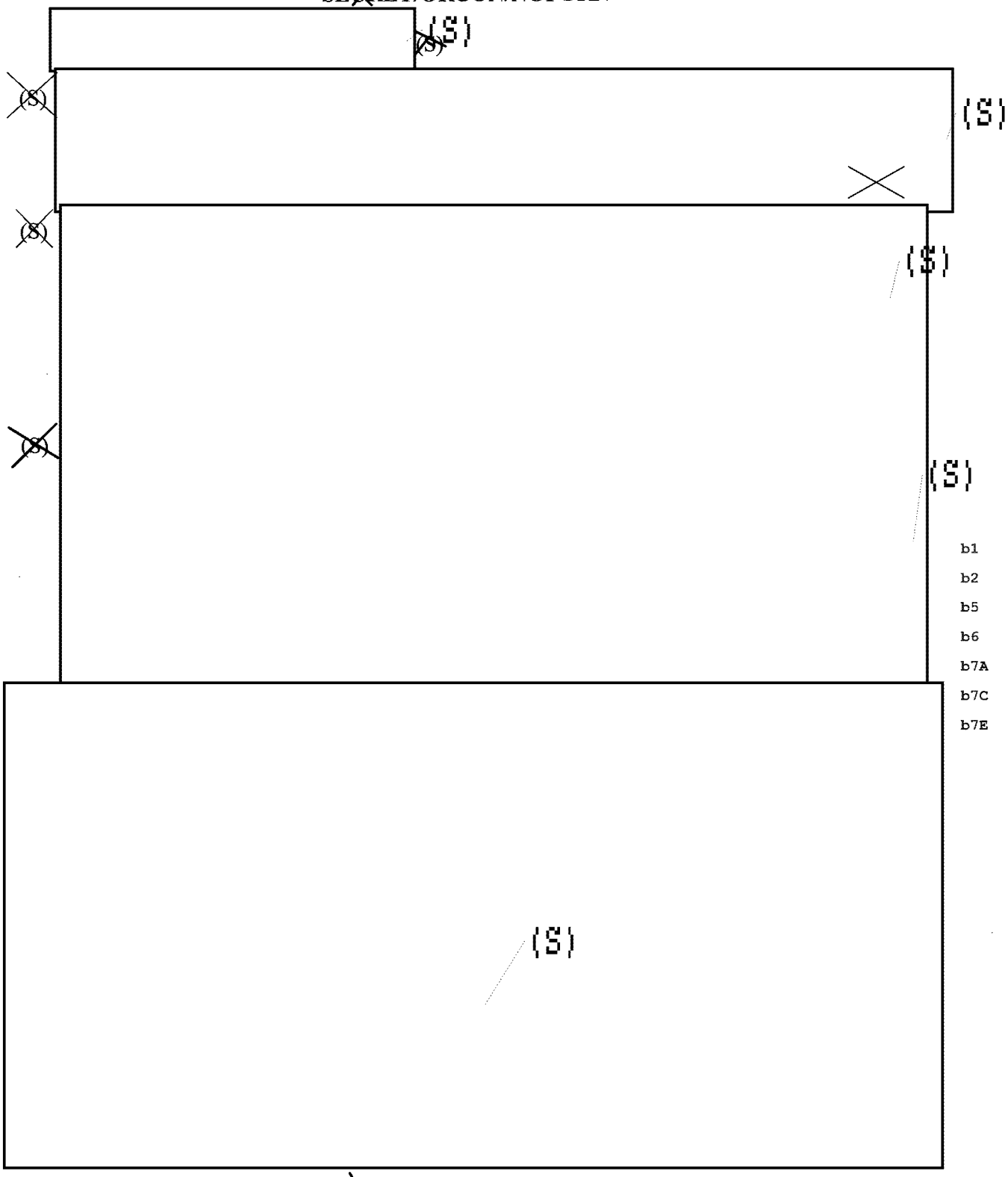
(S)

(S)

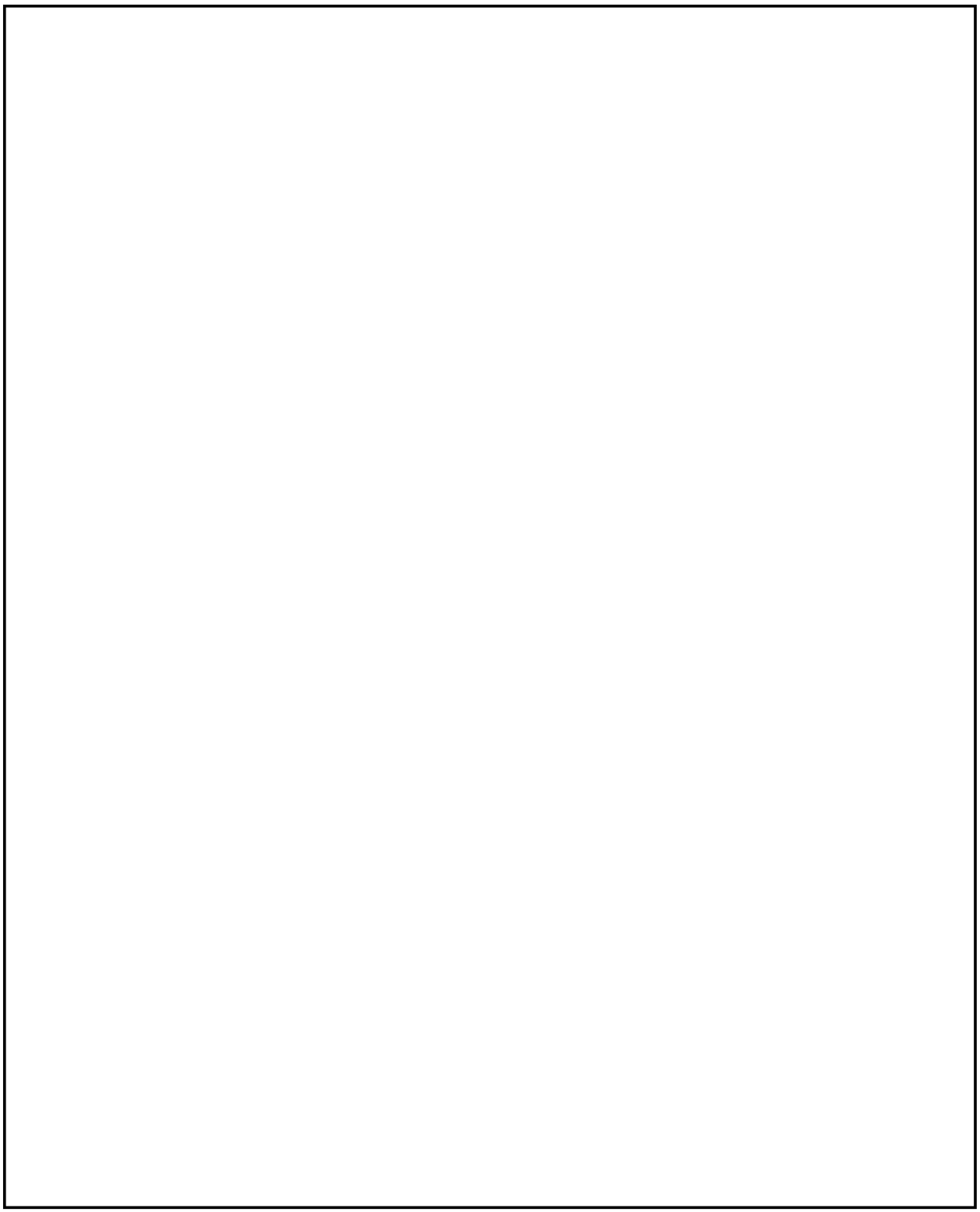


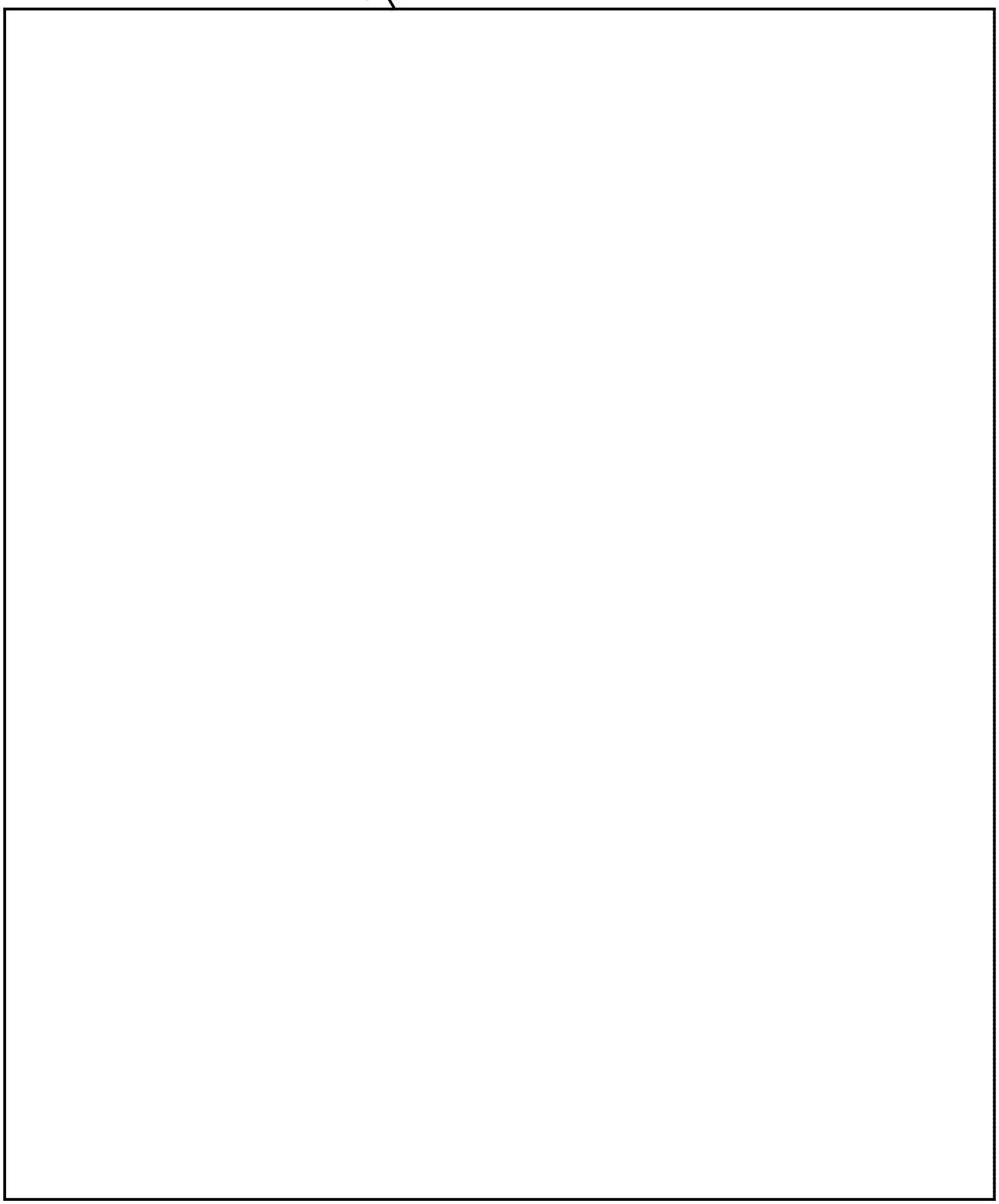



(S)
(S)
(S)



b1
b2
b5
b6
b7A
b7C
b7E





(U)

(U)

(U)

(U)

b1
b2
b5
b7A
b7D
b7E

(U)

(U)

(U)

(S)

(S)

(S)

(S)

(S)

(S//NF,OC)

(S)

b1
b2
b5
b7E

(S)

(U)

(U)

(U)

(S)

(S)

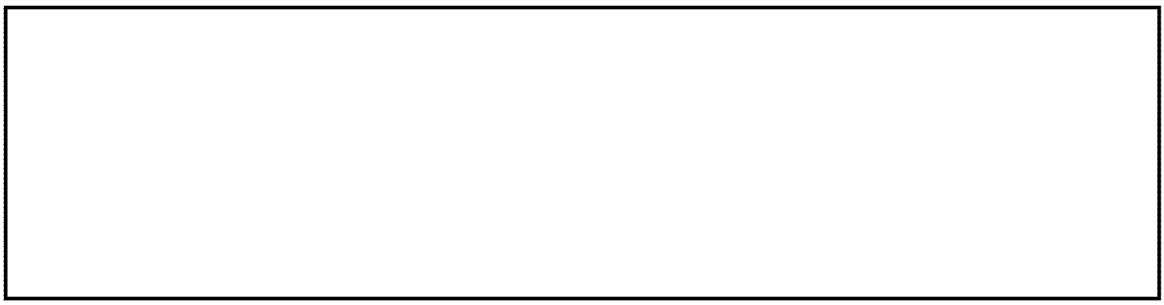
(LES)

(U)

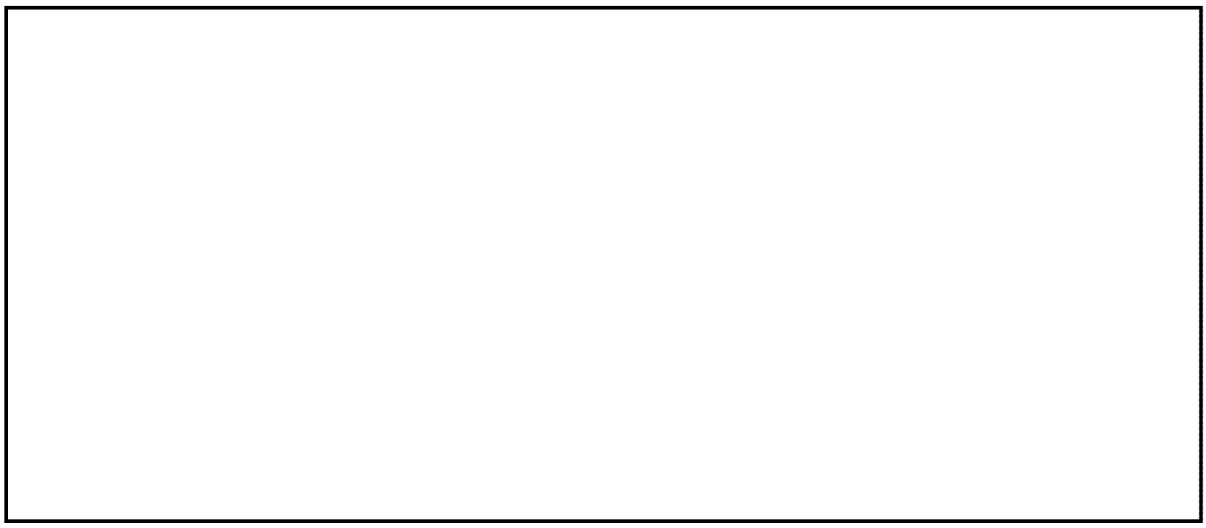
(U)

(U)

(U)



b5



Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. (Wiretap info)

Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. (Catch all - non-wiretap, non-6(e))

EXAMPLES

b2
b7A
b7E

b1
b2
b7E
(S)

b2
b7E

b2
b7D
b7E

(S)

b1
b2
b6
b7A
b7C
b7E

(S)

[redacted]

[redacted] initiated an investigation partially predicated upon information [redacted] b7A b6 b7C

[redacted]

Due to the significance of some of the intelligence information in cited matter an [redacted] b7A b6 b7C

[redacted] b2 b7E

[redacted] b6 b7C

[redacted]

b2 b7E

Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

Prior to the Patriot Act, federal statutes governing the use of criminal investigative wiretaps stated that the interception of wire or oral communications for foreign intelligence purposes should be governed by the provisions of the Foreign Intelligence Surveillance Act (FISA), rather than Title III. This provision, however, did not refer to electronic communications. As a result, it was arguably unclear whether the interception of electronic communications, such as e-mail messages, for foreign intelligence purposes was governed by FISA or Title II (or both). Section 204 clarified the uncertainty by amending Title 18 to confirm that in foreign intelligence investigations, it is FISA, and not Title III, that governs the interception of electronic communications as well as wire and oral communications.

EXAMPLES

b2
b7A
b7E

b2
b7E

Section 206 - Roving FISA Surveillance

When a FISA target's actions have the effect of thwarting surveillance,

b5

DOJ has not declassified the number of requests for roving surveillance authority.

(S)

b1
b2
b7E

Section 207 - Extended Duration for Certain FISAs

b5

Section 207 extends the standard duration for several categories of FISA orders.

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail. The language in Section 209 of the Patriot Act eliminated the distinction in the definitions for "wire communication" and "electronic communication" that was relied on in a 2004 First Circuit opinion (United States v. Councilman) to minimize privacy protection for e-mail. As such, should Congress allow this provision to sunset, it may be unintentionally signaling to the First Circuit and other courts that Congress intends to reduce the privacy protection for e-mails in transit.

EXAMPLES

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury.

EXAMPLES

National Science Foundation's South Pole Station

In May of 2003, the WFO Cyber Squad conducted an investigation involving the computer hacking of the National Science Foundation's South Pole Station. Utilizing the Emergency Disclosures of E-mail & Records by ISPs (section 212), the FBI was able to identify and locate the subject who had hacked into the South Pole Station's computer system and obtained access control of various systems, to include the station's life support.

Jared Bjarnason

The section was utilized by the El Paso Division in April of 2004 to arrest an individual threatening to destroy an El Paso mosque. Jared Bjarnason, an El Paso resident, sent an e-mail message to the El Paso Islamic Center on April 18, 2004. In this message, he threatened to burn the Islamic Center's mosque to the ground if hostages in Iraq were not freed within three days. Agents investigating the threat utilized section 212 to expeditiously obtain information from electronic communications service providers, leading to the identification and arrest of Bjarnason before he could harm the mosque. Absent the emergency access afforded by section 212, the Agents would probably not have been able to locate and arrest Bjarnason in time to stop him, were he to carry out his stated threats. Bjarnason pleaded guilty to sending a threatening interstate communication and making a threat against a religious property. He was sentenced to 18 months in federal prison and ordered to complete 150 hours of community service.

Scott Tyree

Section 212 of the PATRIOT Act was utilized to rescue a 13-year old girl who had been lured from her Western Pennsylvania home by a 39-year old man who she met online, and who was holding her captive at his residence in Virginia.

Scott Tyree was a 38 year old divorced 300 pound computer analyst who spent his free time trolling the internet for young teenage girls who he wanted to make his sex slave. Tyree's screen name was "master for teen slave girls."

Unbeknownst to her parents, a 13 year old Pittsburgh girl began chatting online with Tyree in December, 2001. Tyree exploited this young girl's vulnerabilities and befriended her on the internet. After a month of chatting, Tyree convinced the girl that she should come and live with him in his home in Virginia. He drove to Pennsylvania to pick her up on 01/01/2002.

On 01/02/2002, FBI Pittsburgh received a report from the Pittsburgh Bureau of Police that a 13-year old girl had disappeared from her parents' home on the previous day. FBI agents interviewed the parents and the victim's friends, one of whom reported that the victim had been talking about leaving Pittsburgh with a man she met online. Her computer was examined, but it had been wiped clean. Over the next two days, agents and police officers searched for clues to this child's whereabouts, without any luck.

A break came the evening of 01/03/2002, when the FBI received an anonymous call from a man in Florida who claimed that he had an online friend who lived in Northern Virginia who claimed that he had taken a girl from Pittsburgh to make her his sex slave. The Florida man told the FBI he saw a video, via a live web camera broadcast, of the girl. The girl was naked, and, according to the online friend, had just been beaten. The caller could not recall the screen name used by the man.

On the morning of 01/04/2002, the anonymous caller recontacted the FBI and advised that the suspect used the screen name "master for teen slave girls @ yahoo. com." FBI agents immediately tried to contact Yahoo to find out who this person was. Because Yahoo is based on California and it was the middle of the night, Pacific time, Pittsburgh agents had to contact a Yahoo Vice President at his home in California to trace this screen name. Thanks to a provision in the Patriot Act, the Yahoo Vice Present was able to provide identifying information about the screen name without a grand jury subpoena. This provision of the Patriot Act, Section 212, (18 U.S.C. § 2702(b)} allows an Internet Service Provider to immediately provide information to law enforcement in the case of an emergency involving an immediate risk of death or serious bodily injury. As a result of that provision of the Patriot Act, we were able to quickly identify Scott Tyree and find out where he lived. Agents immediately went to Tyree's residence and rescued the child victim, who was found laying nearly naked in a bed, with a collar around her neck, chained to a wall. Tyree was arrested that same day at his place of employment, Computer Associates in Virginia.

We later learned while the child victim was trapped in Tyree's Virginia home for 4 days, that he treated her as his sex slave, physically and sexually abusing her. The child victim was collared and kept chained in Tyree's bedroom or chained in a "dungeon" in his basement, where he kept hundreds of sado masochistic devices.

Tyree eventually pled guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor (18 U.S.C. §§ 2423(b) and 2251(a)) and was thereafter sentenced to a term of 235 months imprisonment.

Section 214 - FISA Pen/Trap Authority

FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications (i.e. Internet), comparable to the criminal pen/trap provision.

EXAMPLES

The total number of orders by the Foreign Intelligence Surveillance Court authorizing the installation and use of pen registers and trap and trace devices for the period of October 26, 2001 through March 31, 2005 has been declassified. The total number is _____.

DOJ has not declassified the number of requests for FISA pen register / trap trace authority.

(S)

b1

(S)

(S)

b2
b7E

Section 215 - Access to Business Records under FISA

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records [redacted] to include "any tangible things (including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

EXAMPLES

The total number of orders approved by the Foreign Intelligence Surveillance Court for access to certain business records for foreign intelligence purposes under this provision from October 26, 2001 through March 31, 2005 has been declassified. The total number is _____.

The number of such order issued to libraries and/or booksellers from October 26, 2001 through March 31, 2005 has been declassified. The total number is _____.

The categories of information that have been sought to date in orders for the production of tangible things under Section 215 of the Act, specifically:

1) [redacted]
2)
3)
4)
5)

b2
b7E

DOJ has not declassified the number of requests for FISA business record orders.

Section 217 - Interception of Computer Trespasser Communications

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

EXAMPLES

The hacker trespasser exception has been an important tool for law enforcement to obtain evidence based on the consent of the victim. A diverse array of examples from the Cyber criminal investigations include (a) the FBI's investigation of hackers who took over a local government server in order to collect credit card and drivers license numbers of victims of a major identity theft phishing scam; (b) the FBI's investigation of hackers who broke into the network of a major Trust, and whose server then became the storage facility for pirated software, movies, and video games; and (c) the joint investigation by the FBI and the [redacted] b7D [redacted] into a hacker who broke into a router used by the United States Supreme Court.

Section 218 - Change in the "Primary Purpose" Standard of FISA

Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk.

EXAMPLES

As stated above, FBI field offices overwhelmingly herald the information sharing provisions as the most important provisions in the USA Patriot Act. Section 218 is an essential component to these changes. This provision allows prosecutors to be involved in the earliest phases of an international terrorism investigation without jeopardizing the use of the FISA technique. AUSAs are often co-located with the JTTFs and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks.

PIJ [redacted] b6 b7C

A limited amount of FISA-derived information was passed over "the wall" prior to the passage of the Patriot Act for use in a pending criminal investigation of the worldwide leadership of the Palestinian Islamic Jihad (PIJ), a designated foreign terrorist organization. Prior to the passage of the Patriot Act, an indictment was being prepared, based in part on this FISA-derived information. When the "wall" came down, voluminous information was passed to the criminal investigators and prosecutors giving them a much clearer understanding of the case. As a result, a superseding indictment was filed on the case on [redacted]

Prior to the passage of the Patriot Act and prior to "the wall" coming down, [redacted] summaries and [redacted] were selected by intelligence investigators and passed "over the wall" to the criminal investigators assigned to this case. This information was later declassified and utilized in preparing an initial RICO indictment, which was returned on February 19, 2003. After "the wall" came down, the criminal investigators had the opportunity to review all information derived from a series of [redacted] that were in operation over a period of approximately nine years. [redacted] b2 b7E b6 b7C Consequently, new overt acts were developed, existing overt acts were enhanced, and the prosecutive theory of the case became stronger. A superseding indictment was returned on [redacted] which added additional charges and overt acts, streamlined the prosecutive theory, and added another subject who was previously named as an unindicted co-conspirator.

[redacted] investigation and RICO prosecution as a new method of attacking terrorism following the passage of the Patriot Act. The jury trial of [redacted] and others is set to begin on 05/16/2005 in [redacted] Florida.

b6
b7C
b2
b7E

Section 220 - Nationwide Search Warrants for Electronic Evidence

Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

EXAMPLES

INNOCENT IMAGES (S)

Baltimore has utilized th[redacted]imes in connection with its Innocent Images investigation. Baltimore's experience in the use of the nationwide search warrants to obtain e-mail from ISPs has shown that they significantly reduce the time it takes to obtain contents of e-mail accounts, and results in a much more efficient use of agent investigative resources. This reduction in time can allow us to obtain information that would otherwise be lost because of the short amount of time some ISPs maintain customer data. It is foreseeable that the time saved obtaining information through the use of nationwide search warrants could have other benefits. While we can not state with certainty that up to this point the use of a nationwide search warrant definitely prevented an act of child sexual exploitation, because of the reduction in time it takes to obtain e-mail information through the use of a nationwide warrant, it is very conceivable that the use of a nationwide warrant in connection with the Innocent Images investigation could prevent such an act of child exploitation at some point in the future. b1

Scott Tyree (Also example of §212)

Section 220 of the PATRIOT Act was utilized to rescue a 13-year old girl who had been lured from her Western Pennsylvania home by a 39-year old man who she met online, and who was holding her captive at his residence in Virginia.

Scott Tyree was a 38 year old divorced 300 pound computer analyst who spent his free time trolling the internet for young teenage girls who he wanted to make his sex slave. Tyree's screen name was "master for teen slave girls."

Unbeknownst to her parents, a 13 year old Pittsburgh girl began chatting online with Tyree in December, 2001. Tyree exploited this young girl's vulnerabilities and befriended her on the internet. After a month of chatting, Tyree convinced the girl that she should come and live with him in his home in Virginia. He drove to Pennsylvania to pick her up on 01/01/2002.

On 01/02/2002, FBI Pittsburgh received a report from the Pittsburgh Bureau of Police that a 13-year old girl had disappeared from her parents' home on the previous day. FBI agents interviewed the parents and the victim's friends, one of whom reported that the victim had been talking about leaving Pittsburgh with a man she met online. Her computer was examined, but it had been wiped clean. Over the next two days, agents and police officers searched for clues to this child's whereabouts, without any luck.

A break came the evening of 01/03/2002, when the FBI received an anonymous call from a man in Florida who claimed that he had an online friend who lived in Northern Virginia who claimed that he had taken a girl from Pittsburgh to make her his sex slave. The Florida man told the FBI he saw a video, via a live web camera broadcast, of the girl. The girl was naked, and, according to the online friend, had just been beaten. The caller could not recall the screen name used by the man.

On the morning of 01/04/2002, the anonymous caller recontacted the FBI and advised that the suspect used the screen name "master for teen slave girls @ yahoo. com." FBI agents immediately tried to contact Yahoo to find out who this person was. Because Yahoo is based on California and it was the middle of the night, Pacific time, Pittsburgh agents had to contact a Yahoo Vice President at his home in California to trace this screen name. Section 220 was used to obtain search warrants for the internet service providers of Tyree and the child victim.

Agents rescued the child victim, who was found laying nearly naked in a bed, with a collar around her neck, chained to a wall. Tyree was arrested that same day at his place of employment, Computer Associates in Virginia. We later learned while the child victim was trapped in Tyree's Virginia home for 4 days, that he treated her as his sex slave, physically and sexually abusing her. The child victim was collared and kept chained in Tyree's bedroom or chained in a "dungeon" in his basement, where he kept hundreds of sado masochistic devices.

Tyree eventually pled guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor (18 U.S.C. §§ 2423(b) and 2251(a)) and was thereafter sentenced to a term of 235 months imprisonment.

Section 223 - Civil Liability for Certain Unauthorized Disclosures

Prior to the passage of the Patriot Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

EXAMPLES

Section 225 - Immunity for Compliance with FISA Wiretap

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISC to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent or a foreign power, such as international terrorists and spies. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers, such as telephone companies or Internet service providers, to carry out such court orders. Prior to the passage of the Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out wiretap and surveillance orders issued by the FISC under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISC without delay.

EXAMPLES

An FBI Special Agent was able to convince an [redacted] to assist in the installation of technical equipment [redacted] pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. The target is an espionage subject. The device has allowed the FBI to track the path of the subject [redacted] This information has been used to understand the subject's routines and his contacts.

b2
b7E

Section 213 - Delayed Notice Search Warrants

Pursuant to section 213, prosecutors can seek a judge's approval to delay notification by making a showing that if notification were made contemporaneous to the search, there is reasonable cause to believe one of the following might occur:

1. notification would reasonably endanger the life or physical safety of an individual;

2. notification would reasonably be expected to cause flight from prosecution;

3. notification would reasonably be expected to result in destruction of, or tampering with, evidence;

4. notification would reasonably result in intimidation of potential witnesses; or

5. notification would reasonably be expected to cause serious jeopardy to an investigation or unduly delay a trial.

EXAMPLES

b1
b2
b6
b7A
b7C
b7E

Several offices have reported the use of the delayed notice provision. The circumstances cited most frequently in these investigations are that notification would reasonably be expected to result in destruction of, or tampering with, evidence and notification would reasonably be expected to cause serious jeopardy to an investigation.

[redacted] (S)

[redacted] (S)

(S)

b1
b2
b6
b7A
b7C
b7E

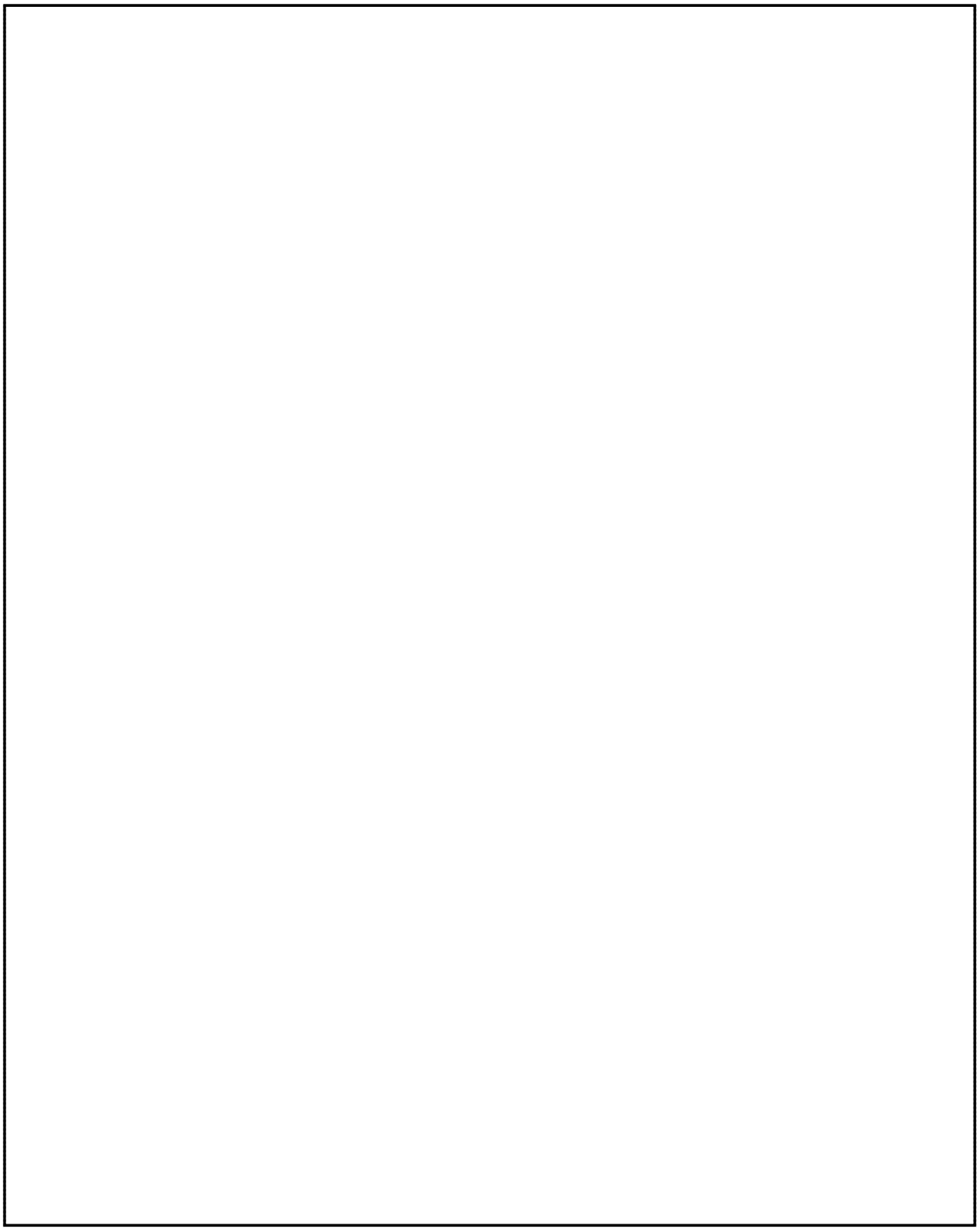
[redacted]

[redacted] (S)

(S)

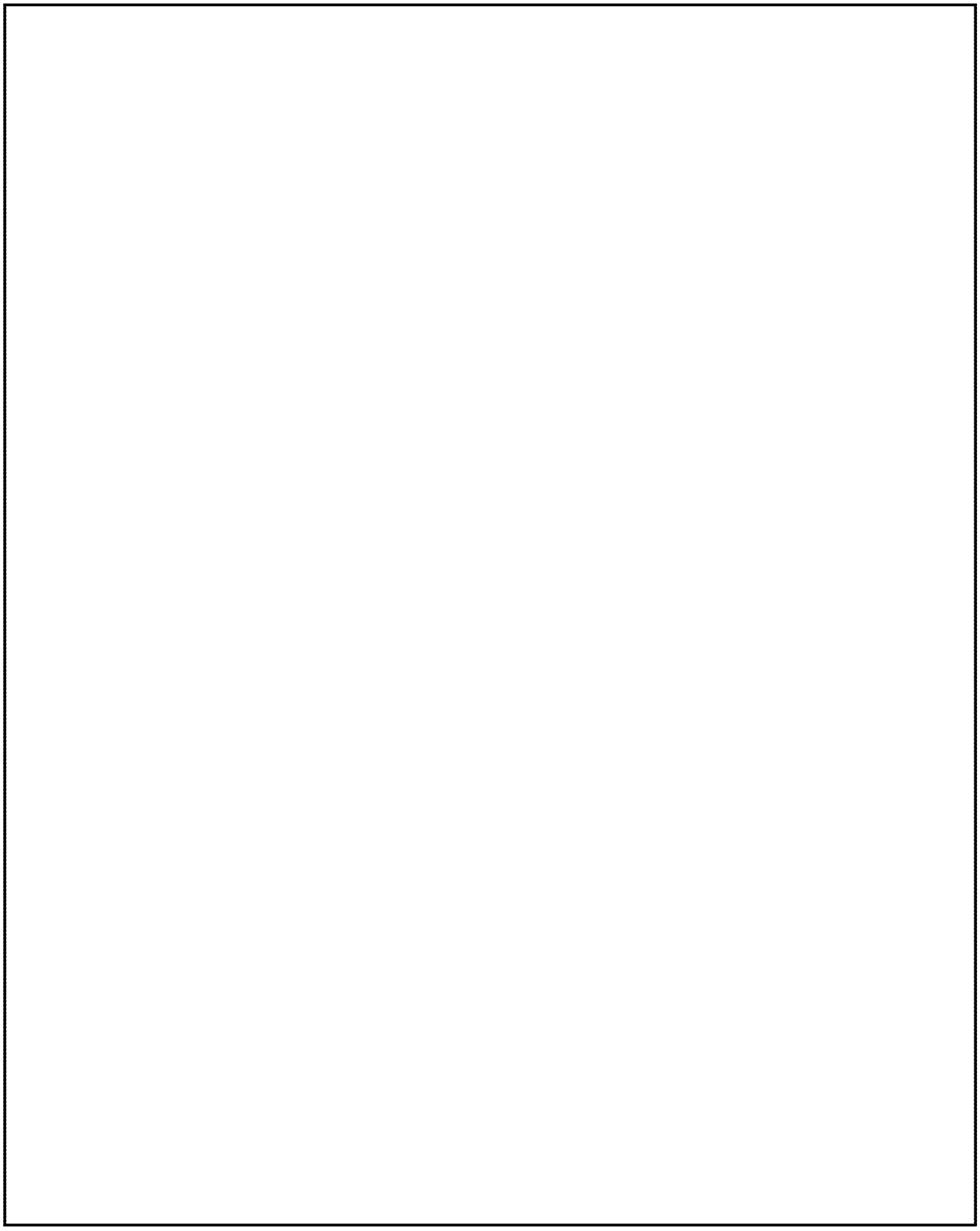
b1
b2
b6
b7A
b7C
b7E

(S)

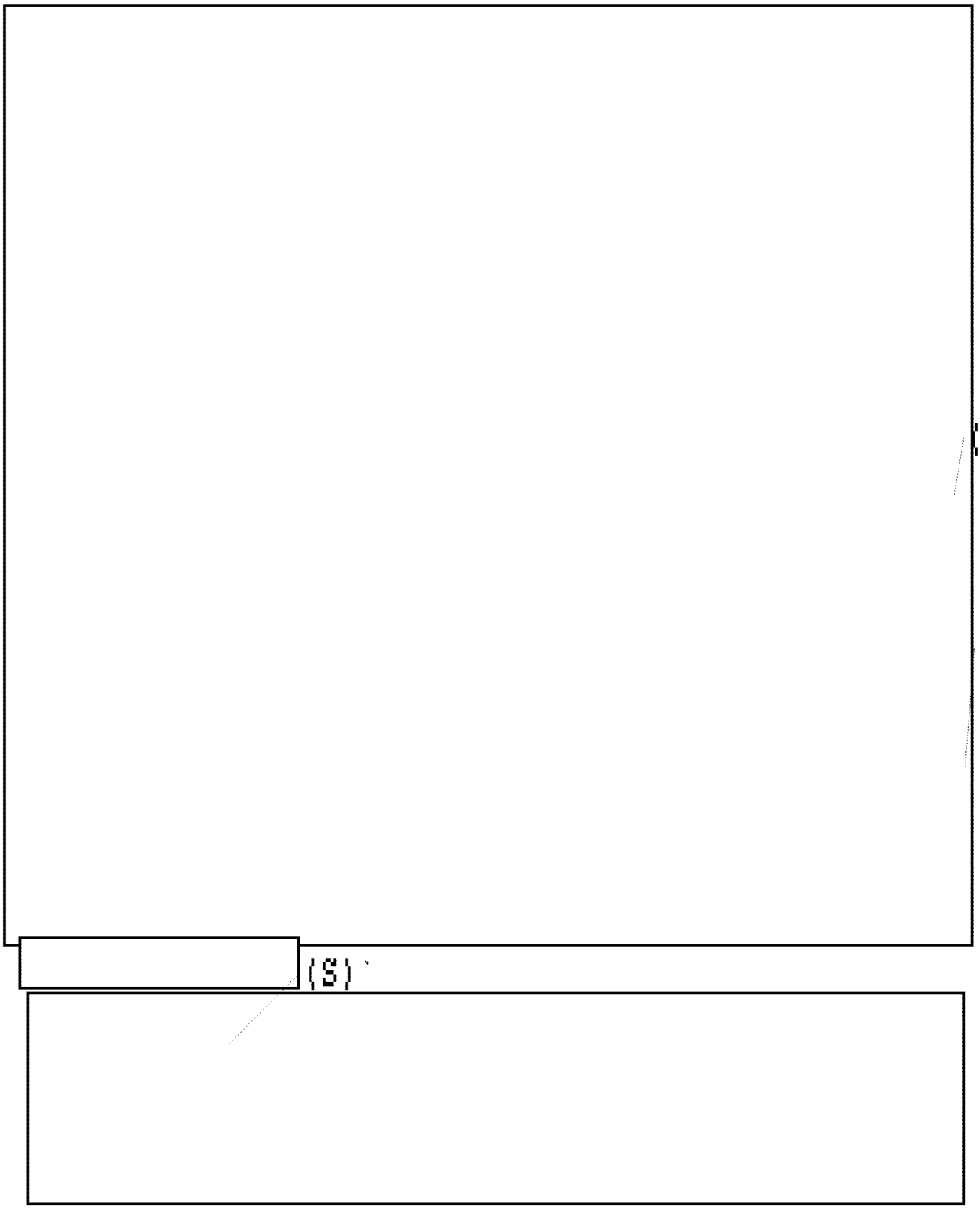


b2
b6
b7A
b7C
b7D
b7E

b6
b7A
b7C



b1
b2
b7E

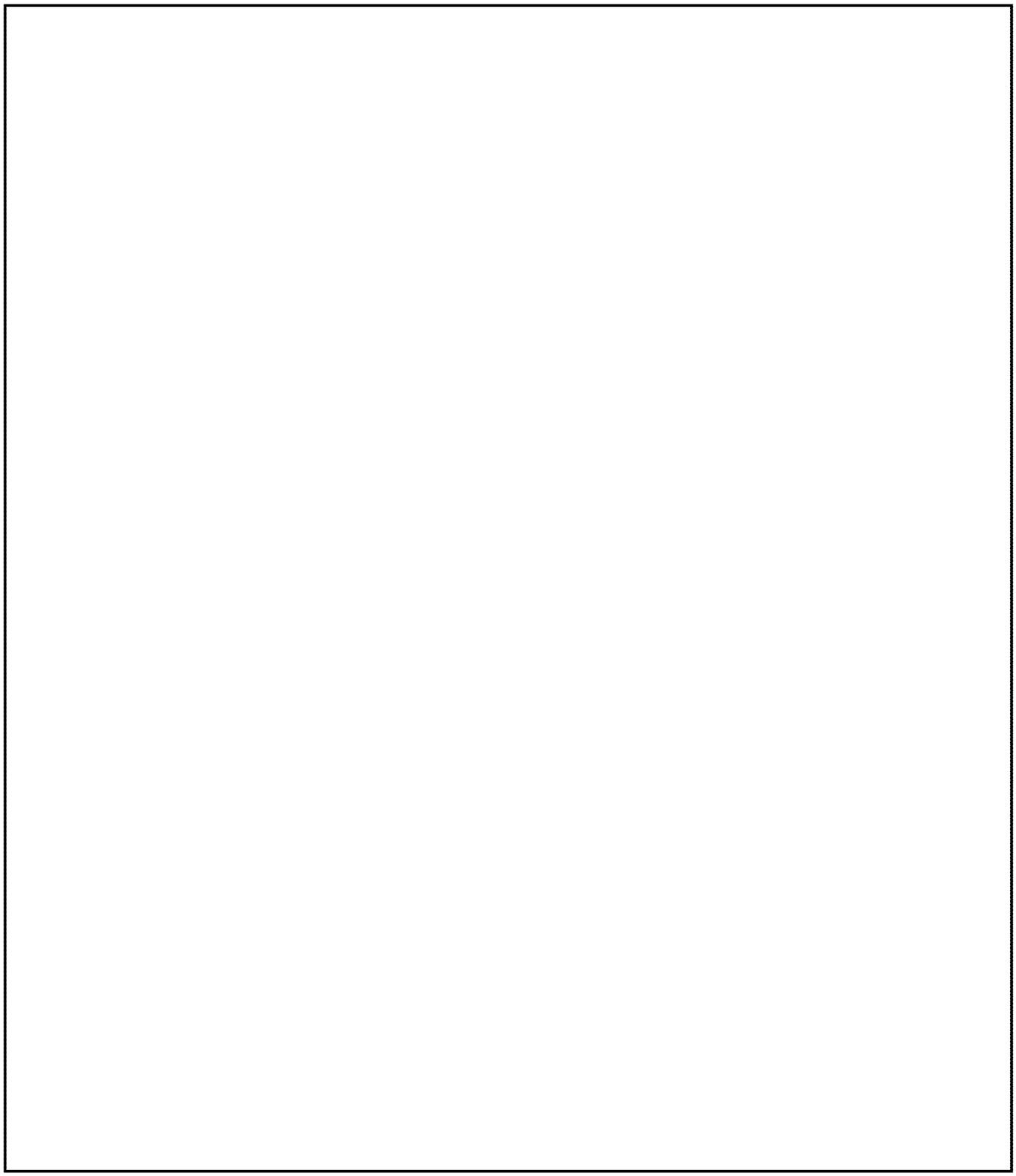


(S)

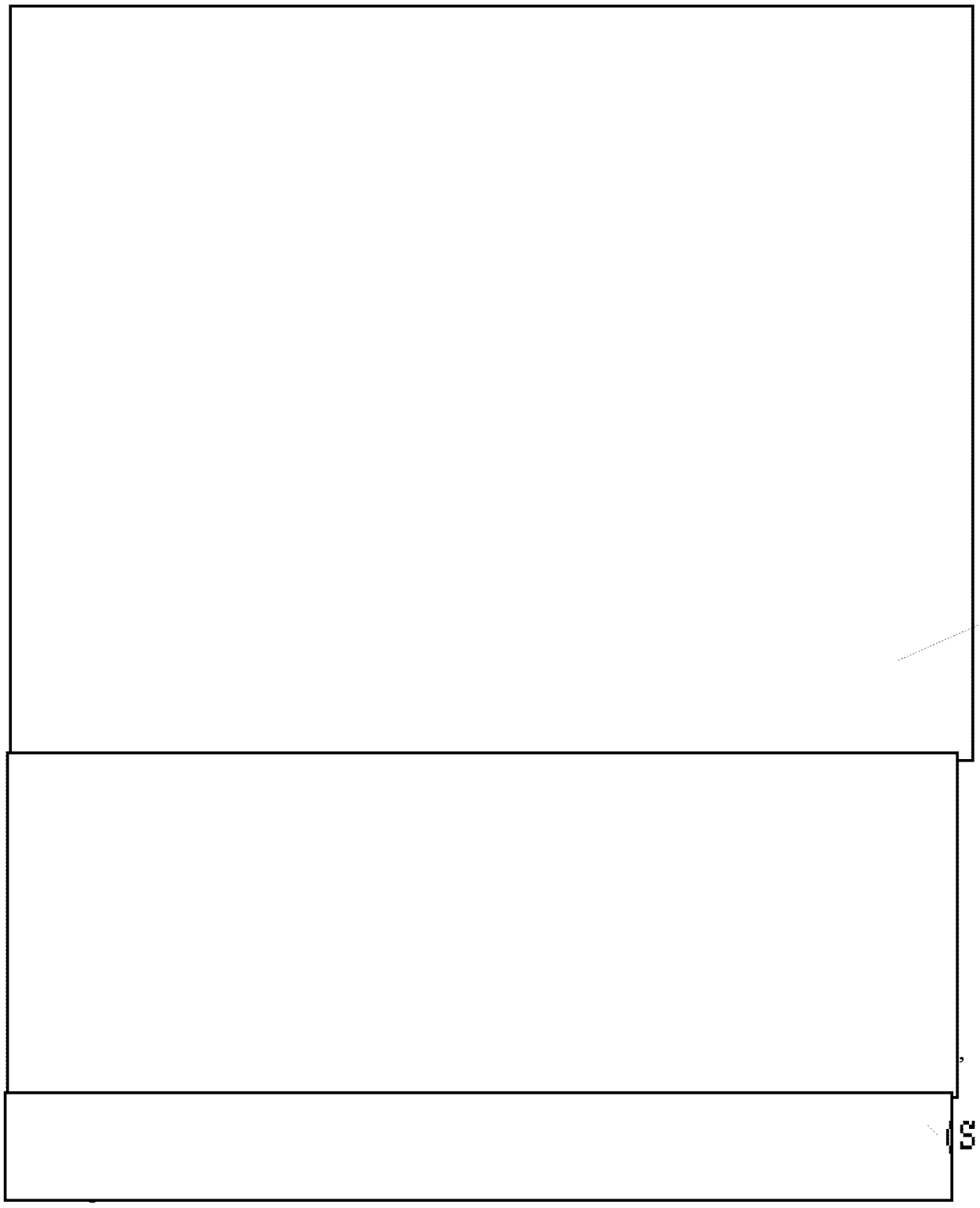
(S)

(S)

b1
b2
b7A



b2
b6
b7A
b7C

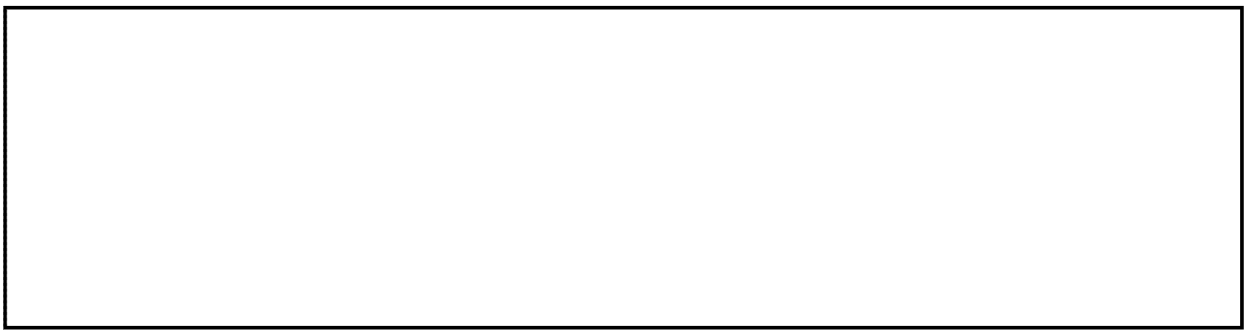


b1
b2
b6
b7A
b7C
b7E

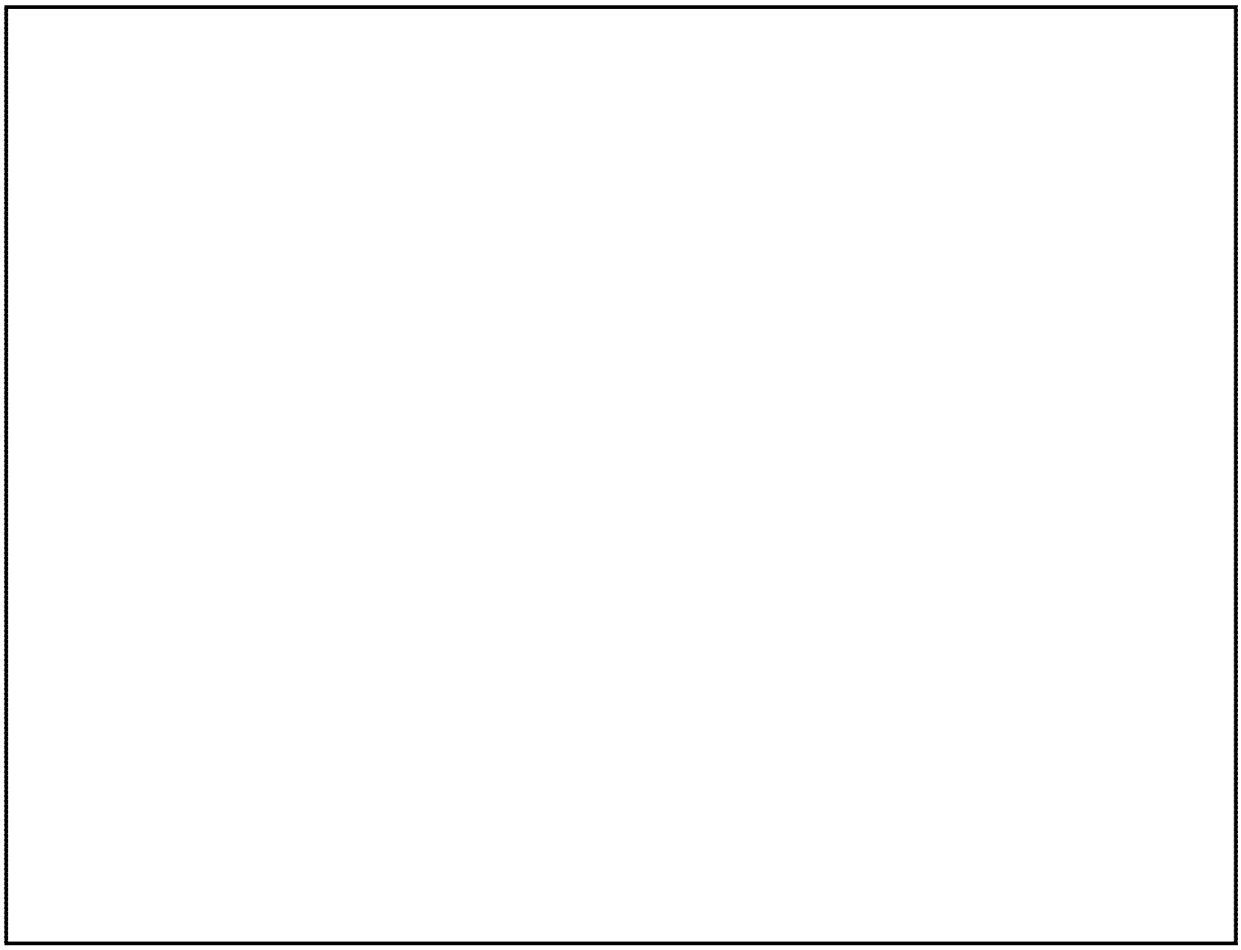
(S)

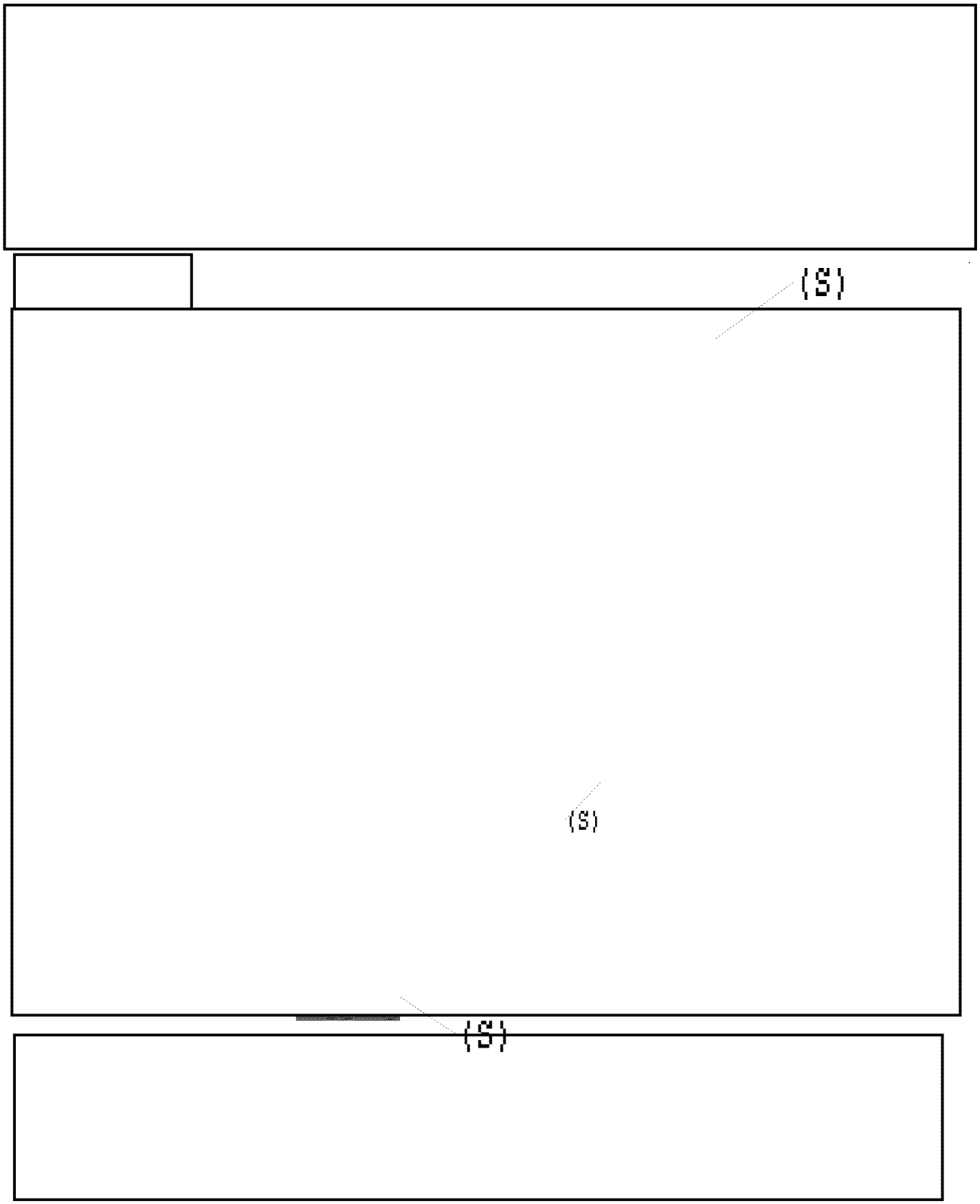
(S)

b5



b6
b7A
b7C

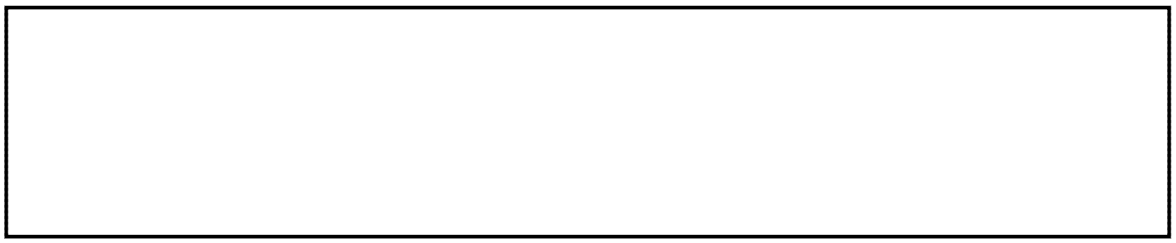




b1
b6
b7A
b7C

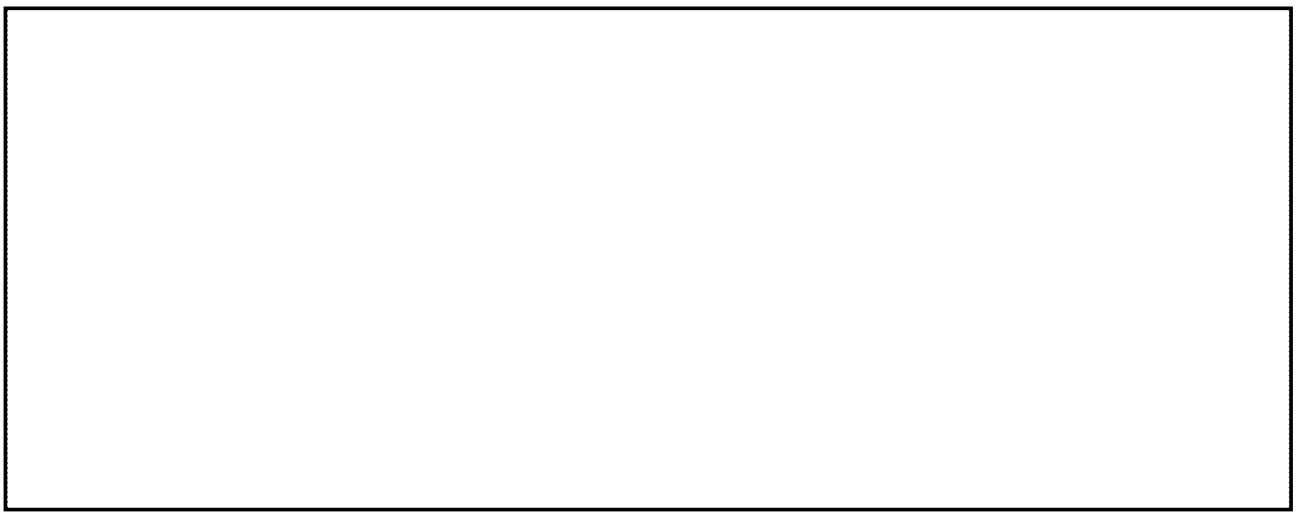
SECRET

b5

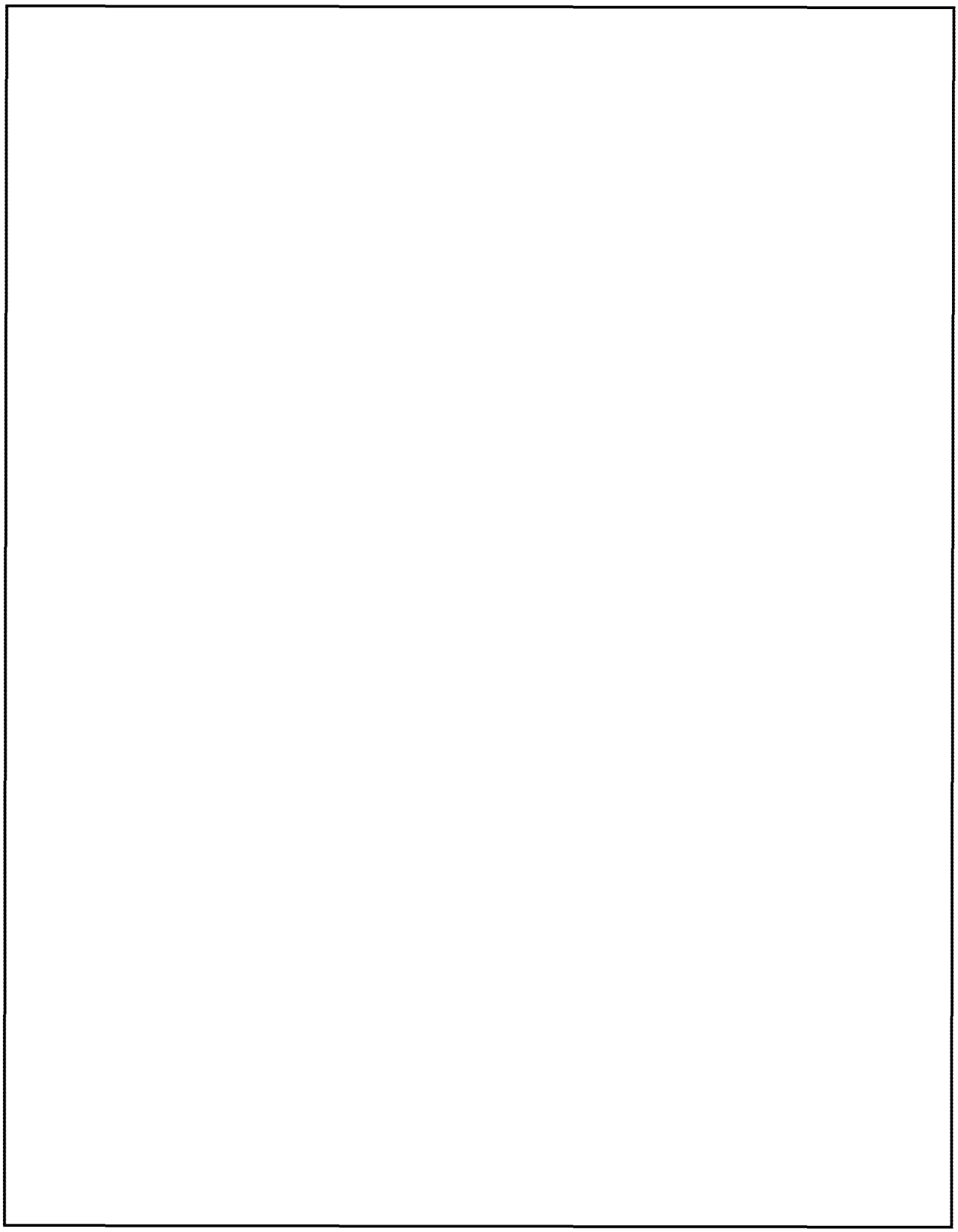


SECRET

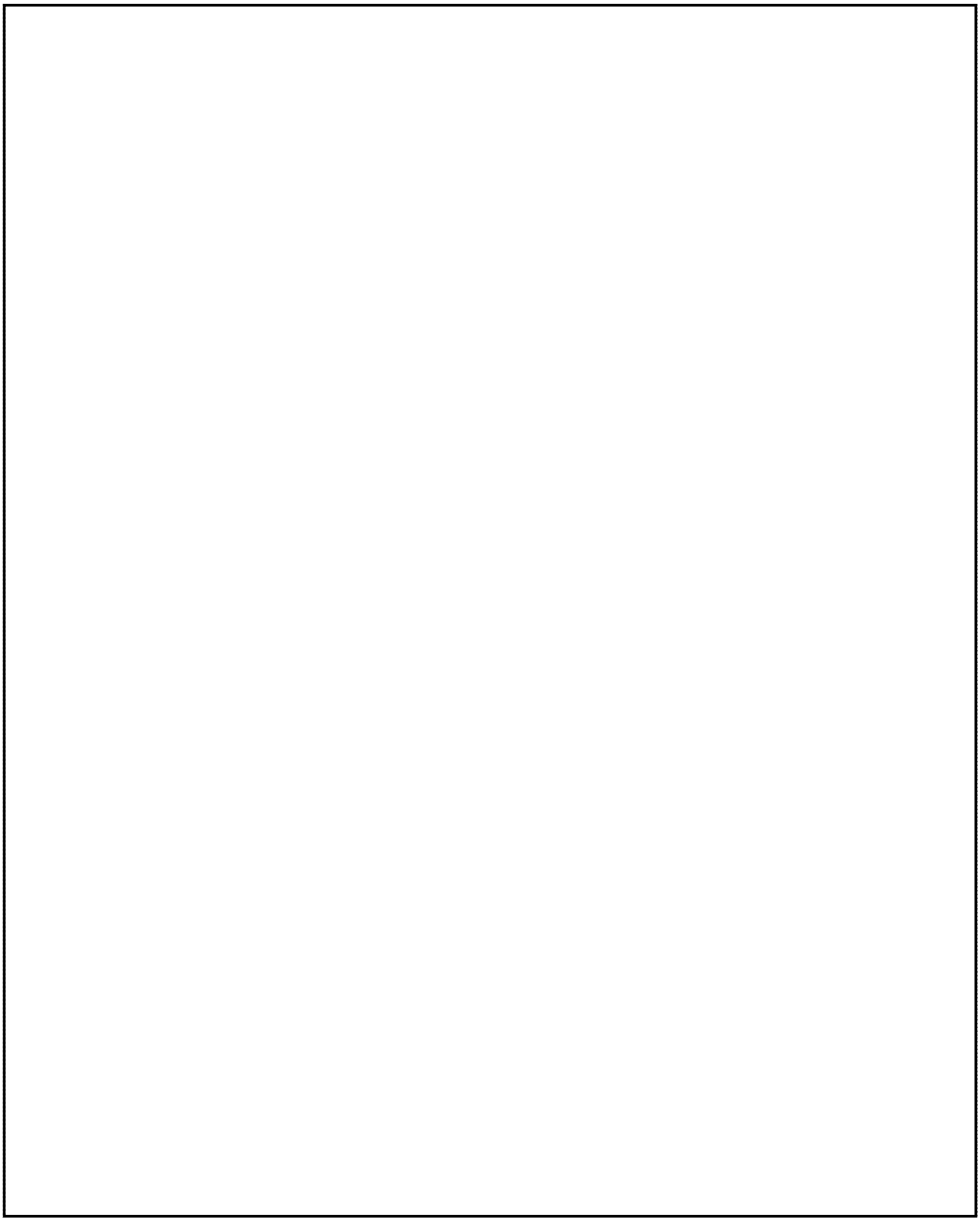
b5



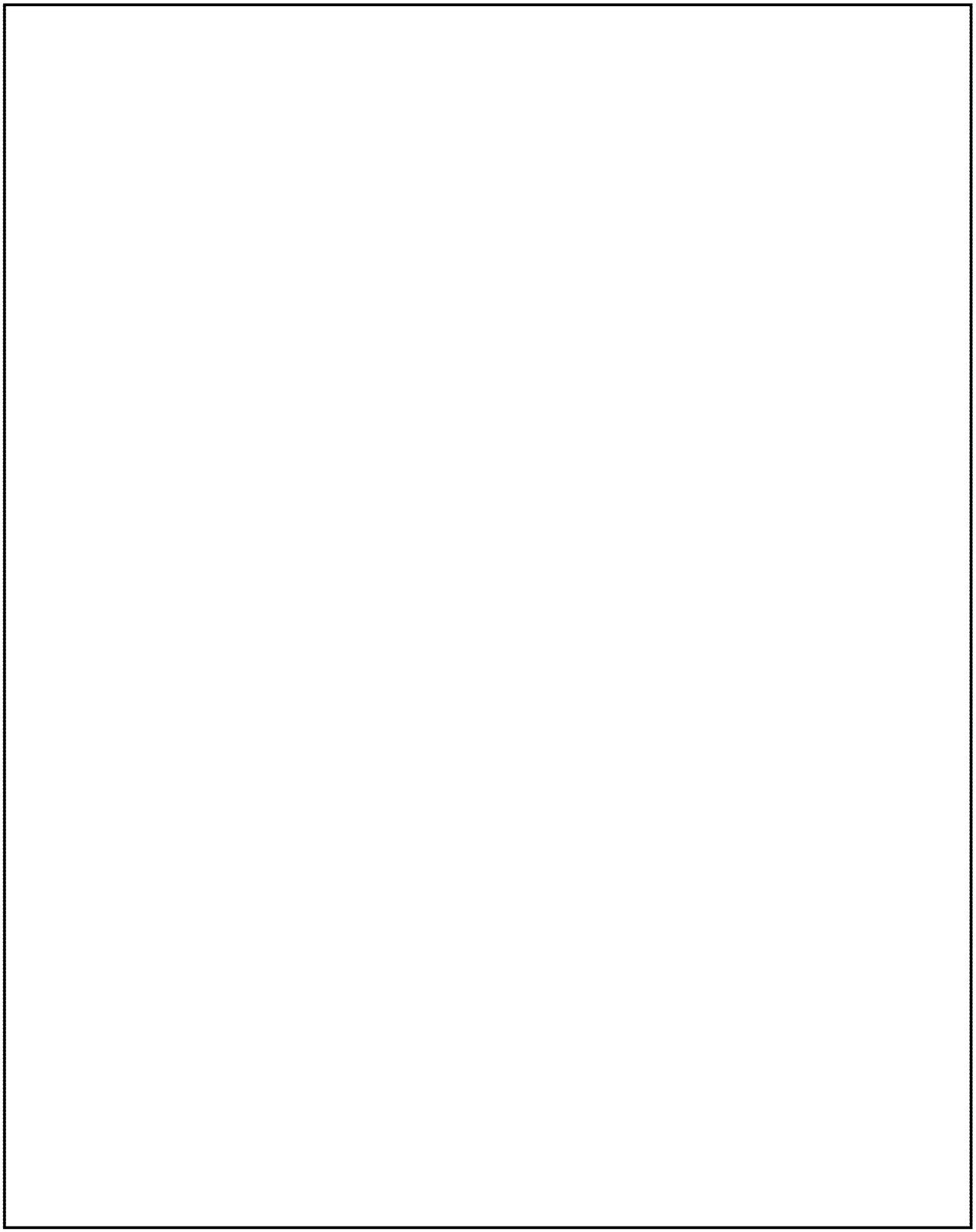
b6
b7A
b7C

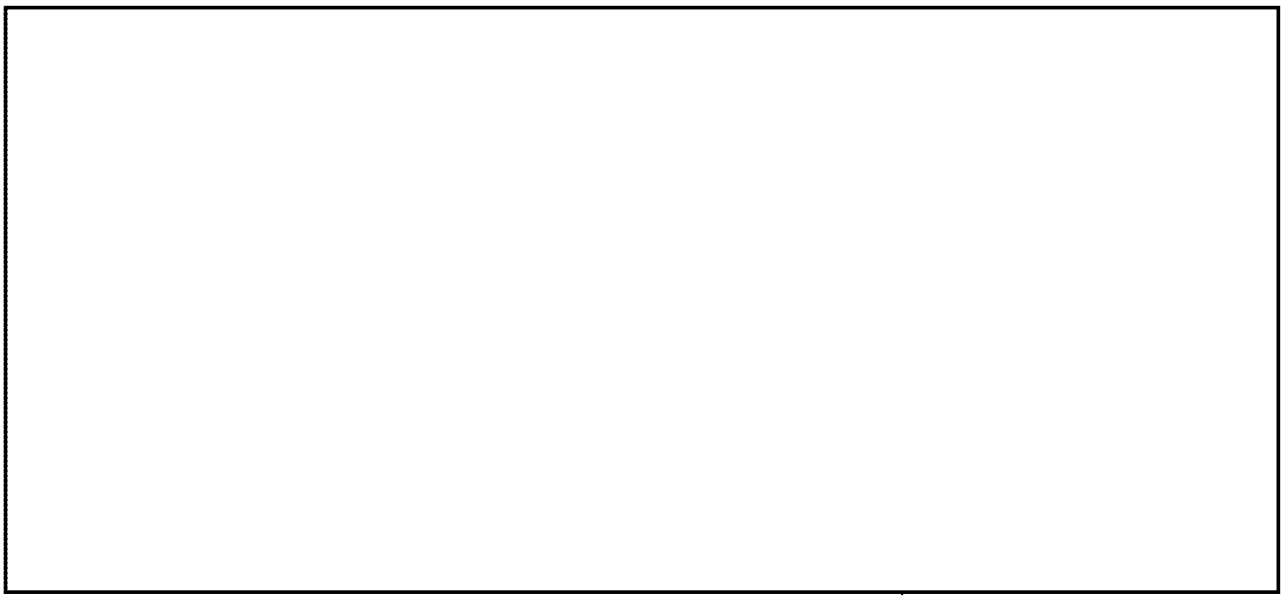


b2
b7A
b7E



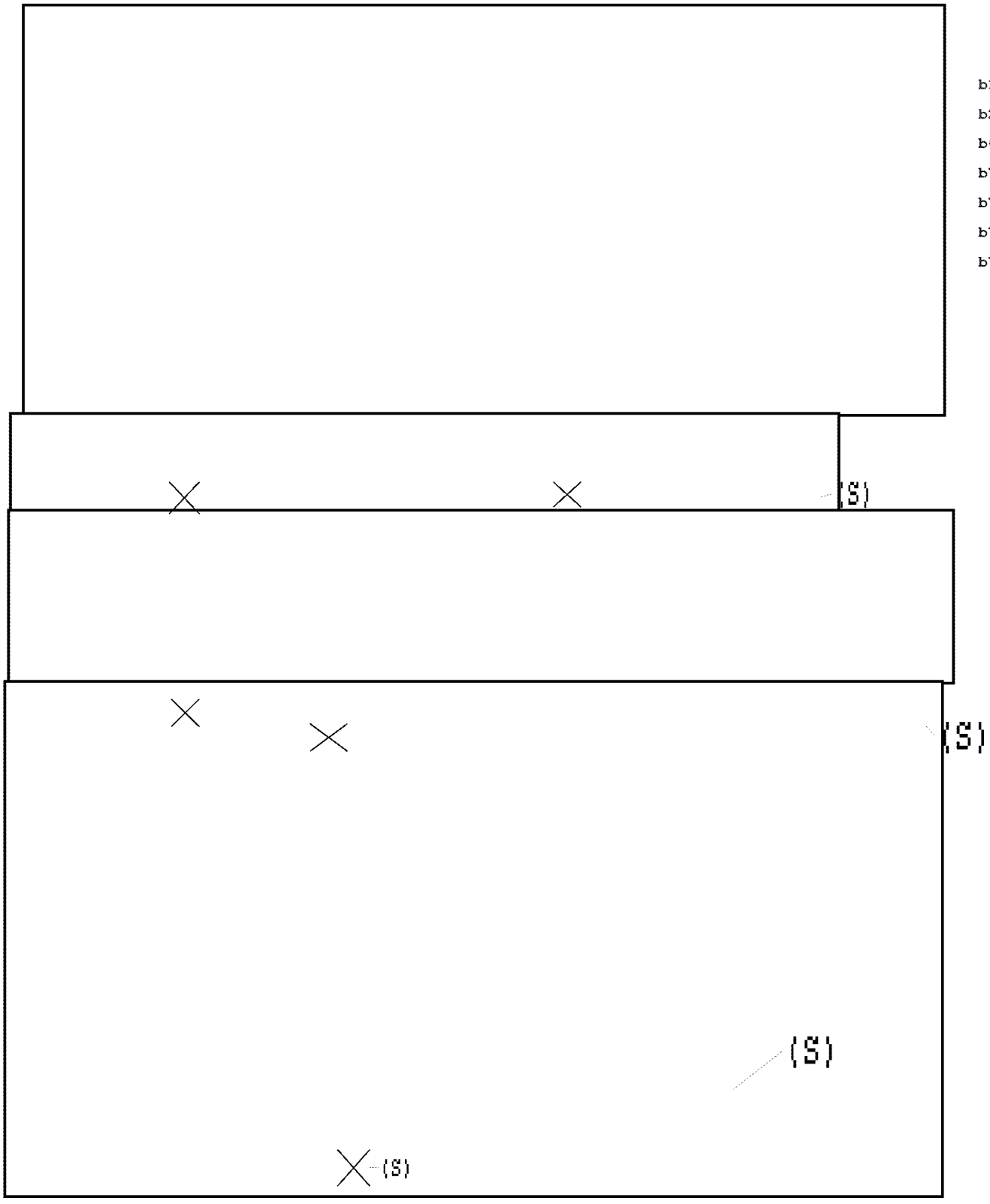
b2
b7A



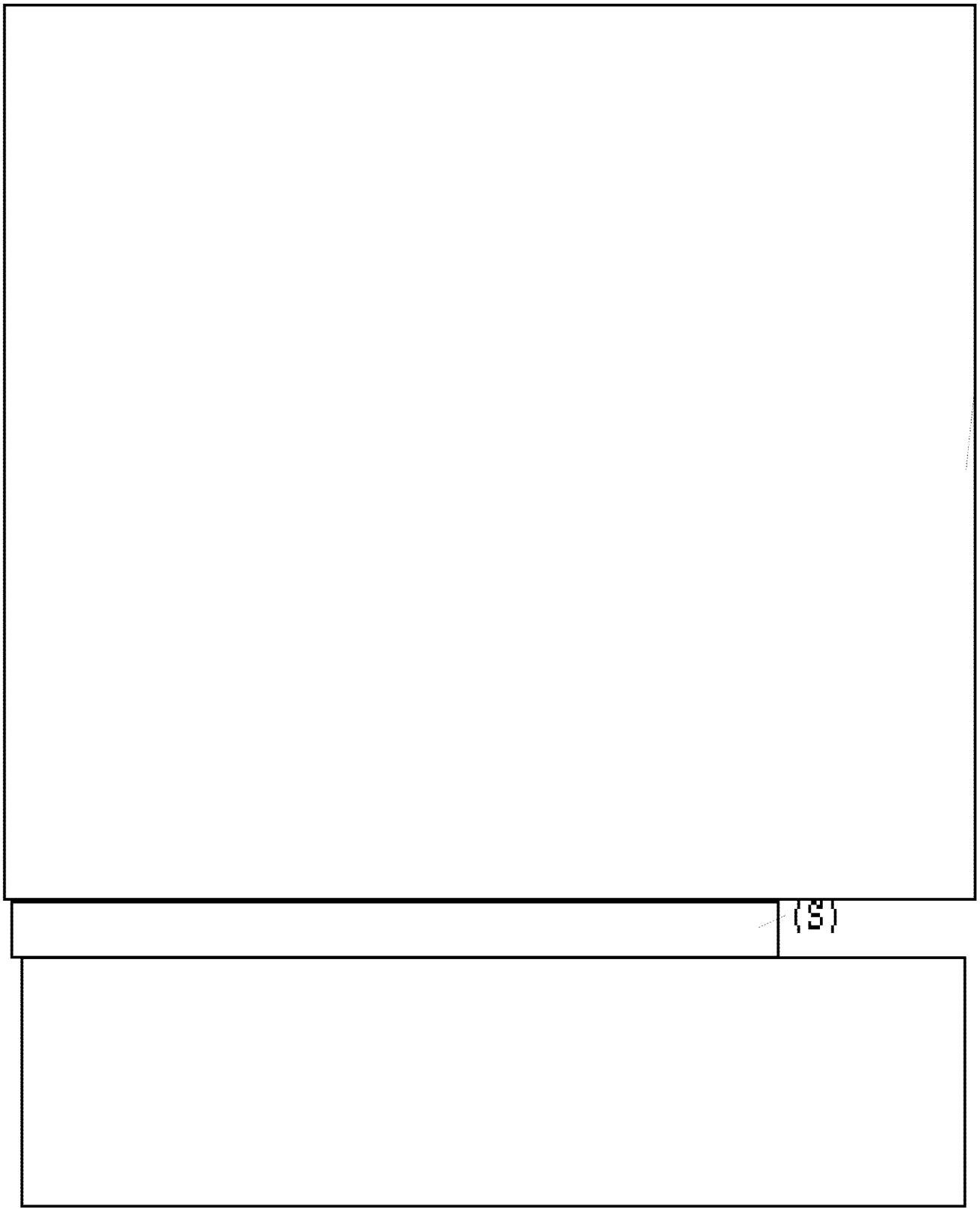


b2
b6
b7C
b7E

b1
b2
b6
b7A
b7C
b7D
b7E

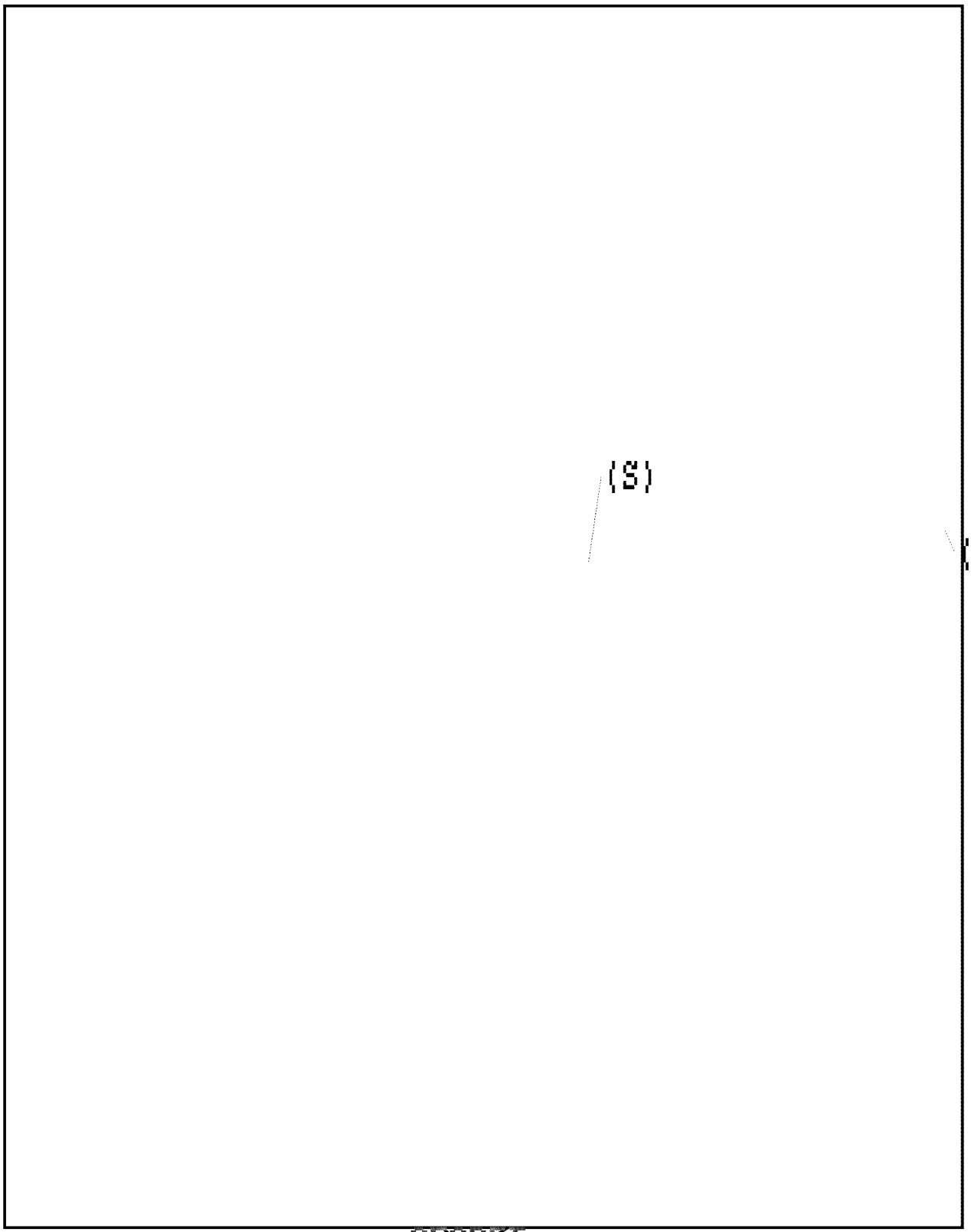


b1
b2
b6
b7A
b7C
b7D
b7E



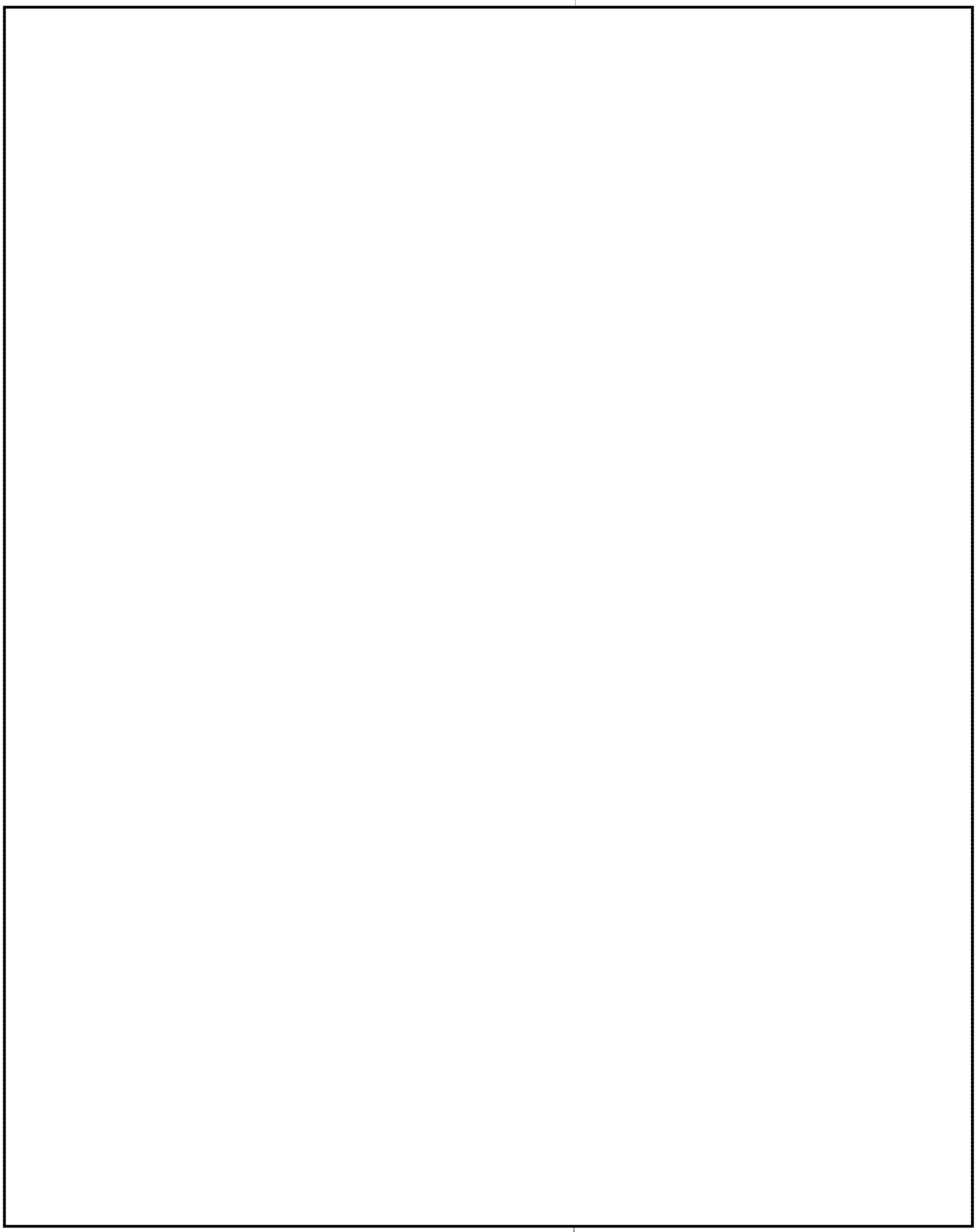
SECRET

b1
b2
b7A
b7E

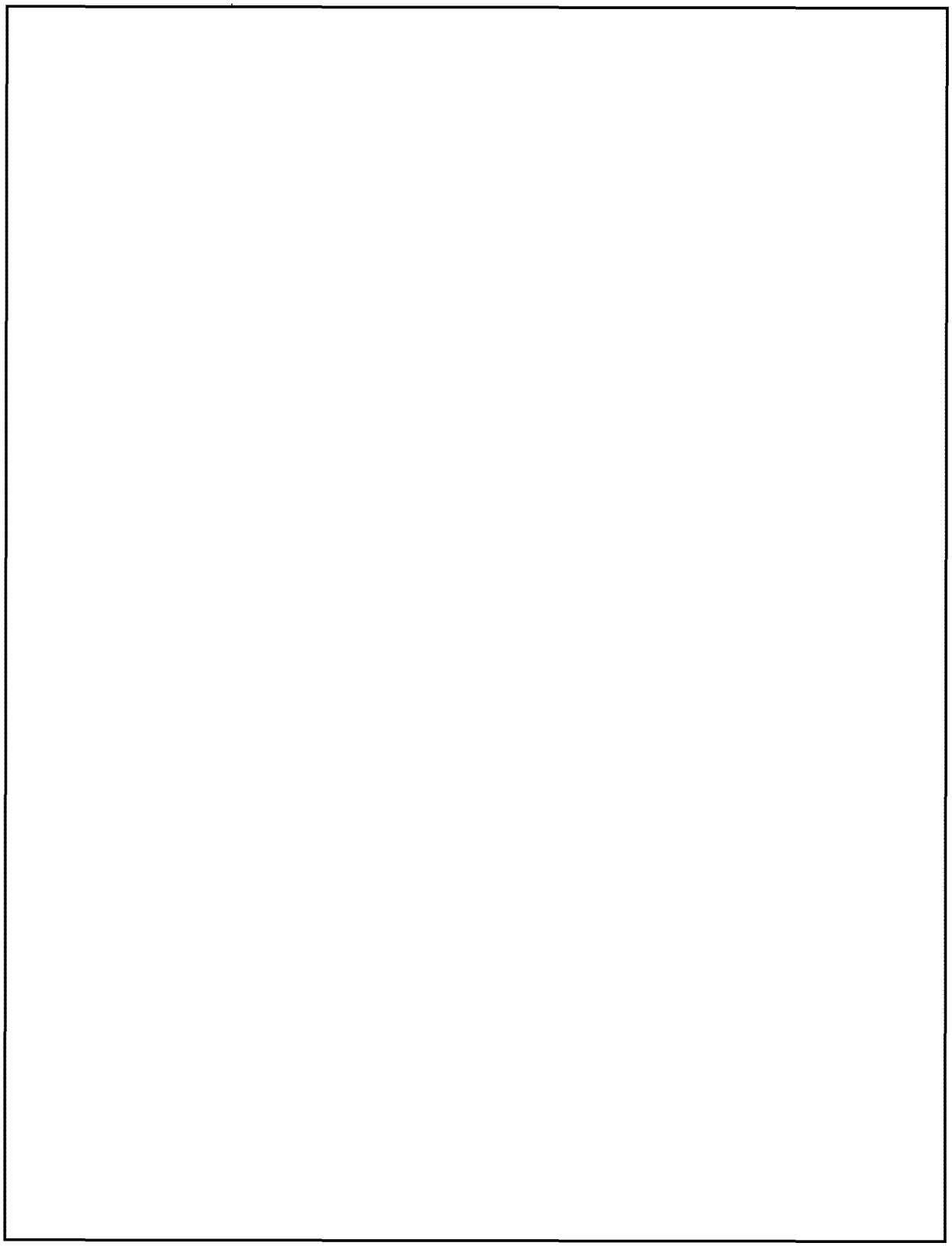


(S)

b1
b2
b7E

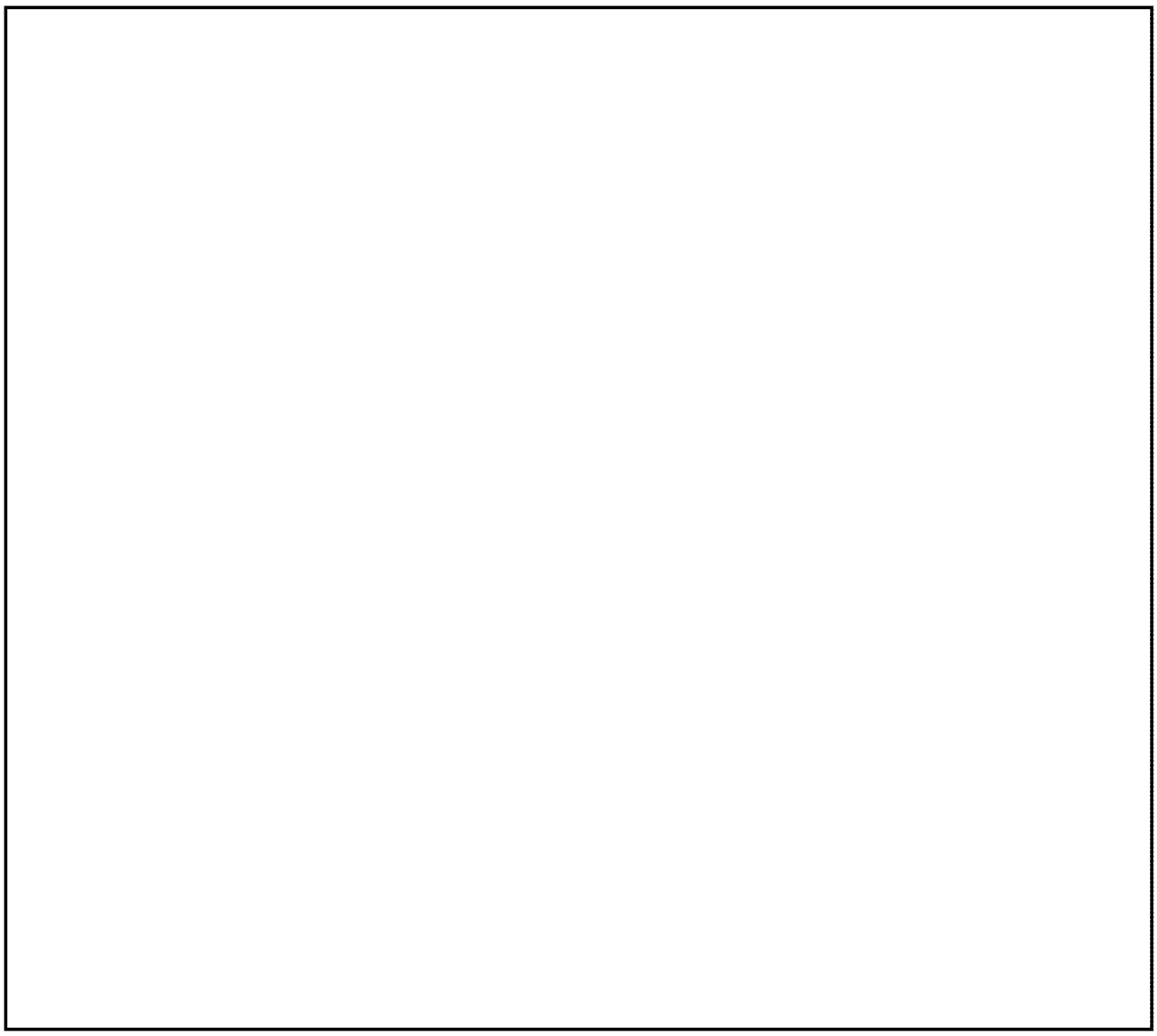


b2
b6
b7C
b7E



b2
b6
b7A
b7C
b7E

b2
b7E

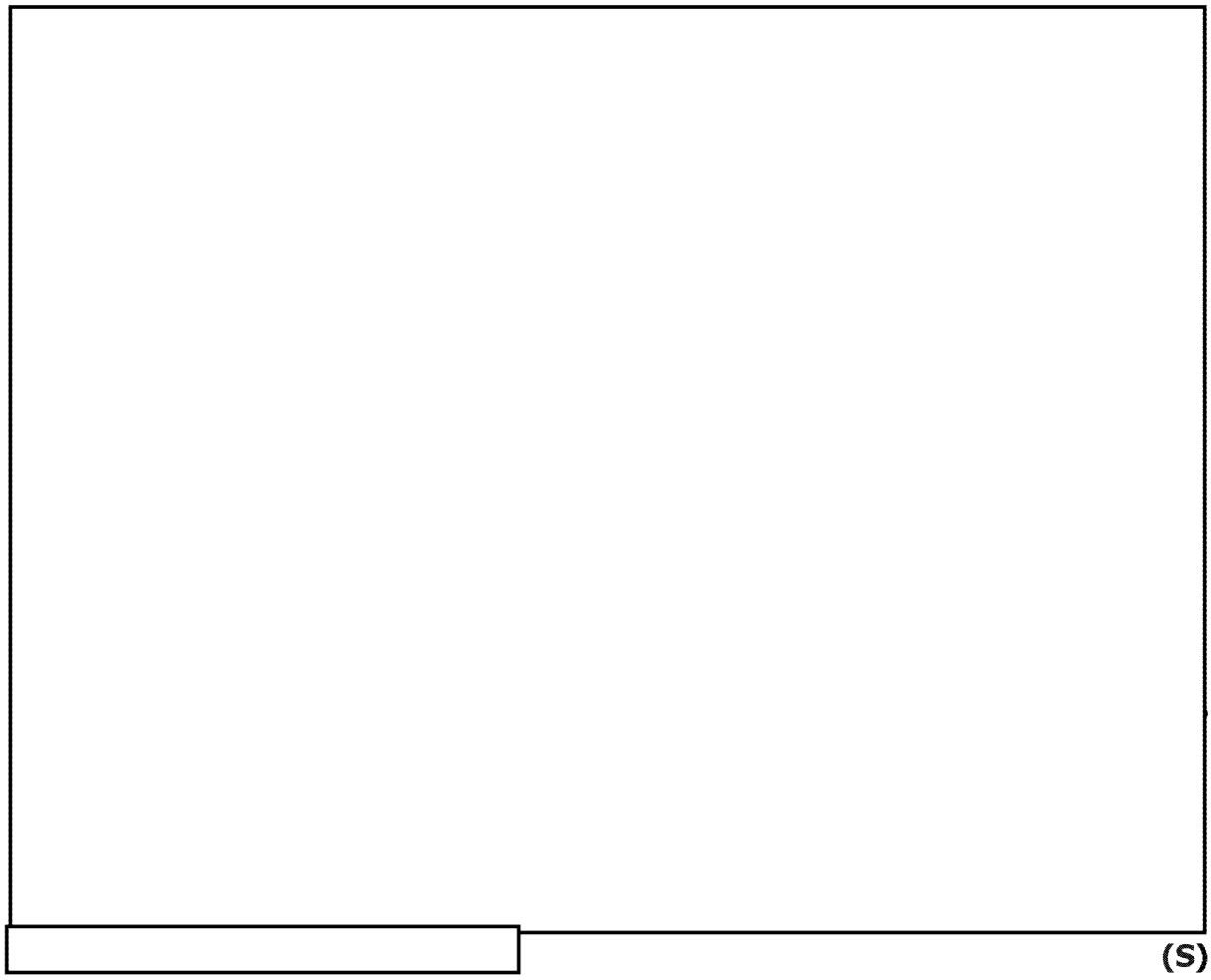


b1
b2
b7A
b7E

Section 218 - Change in the "Primary Purpose" Standard of FISA

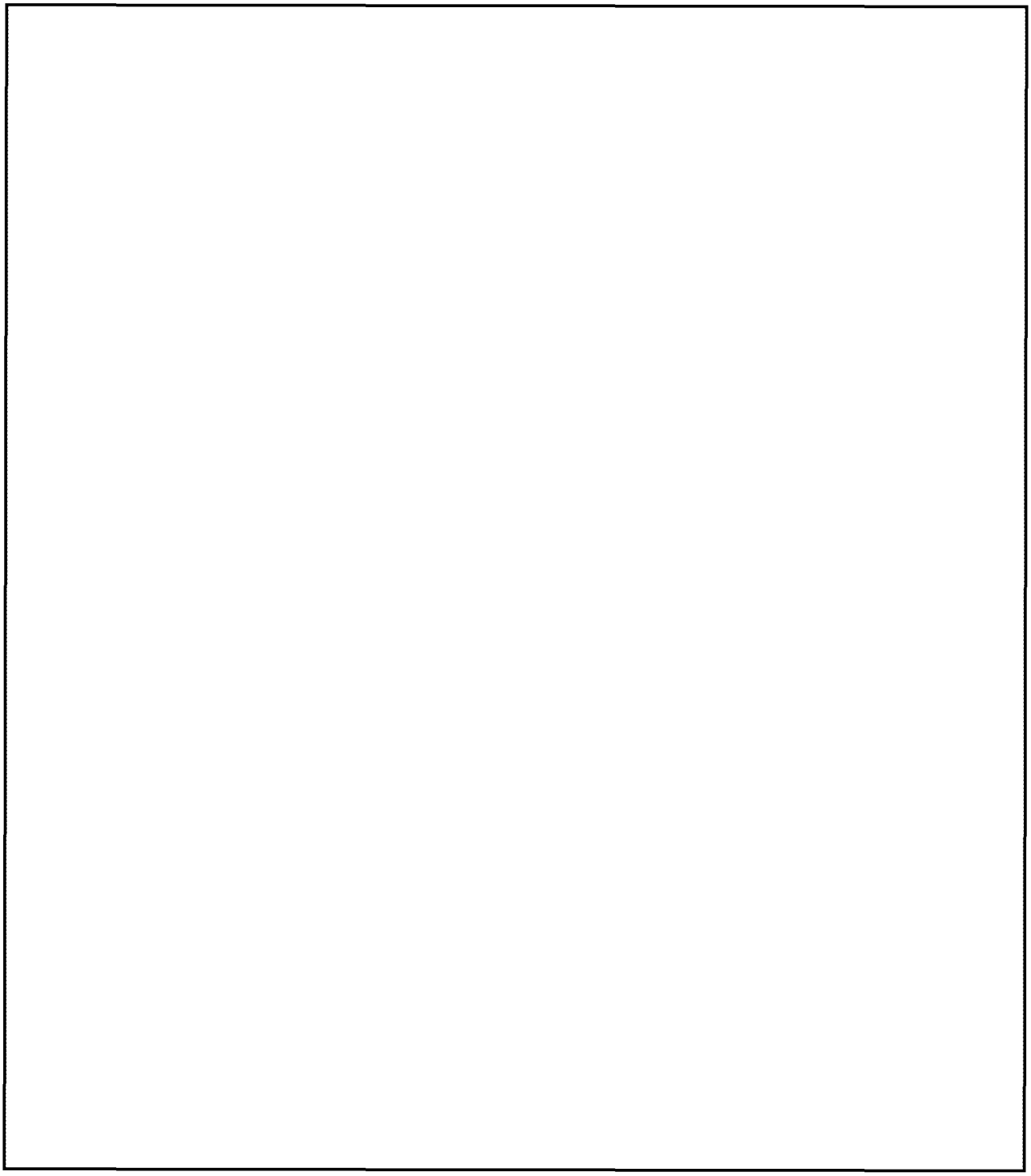
(S)

(S)



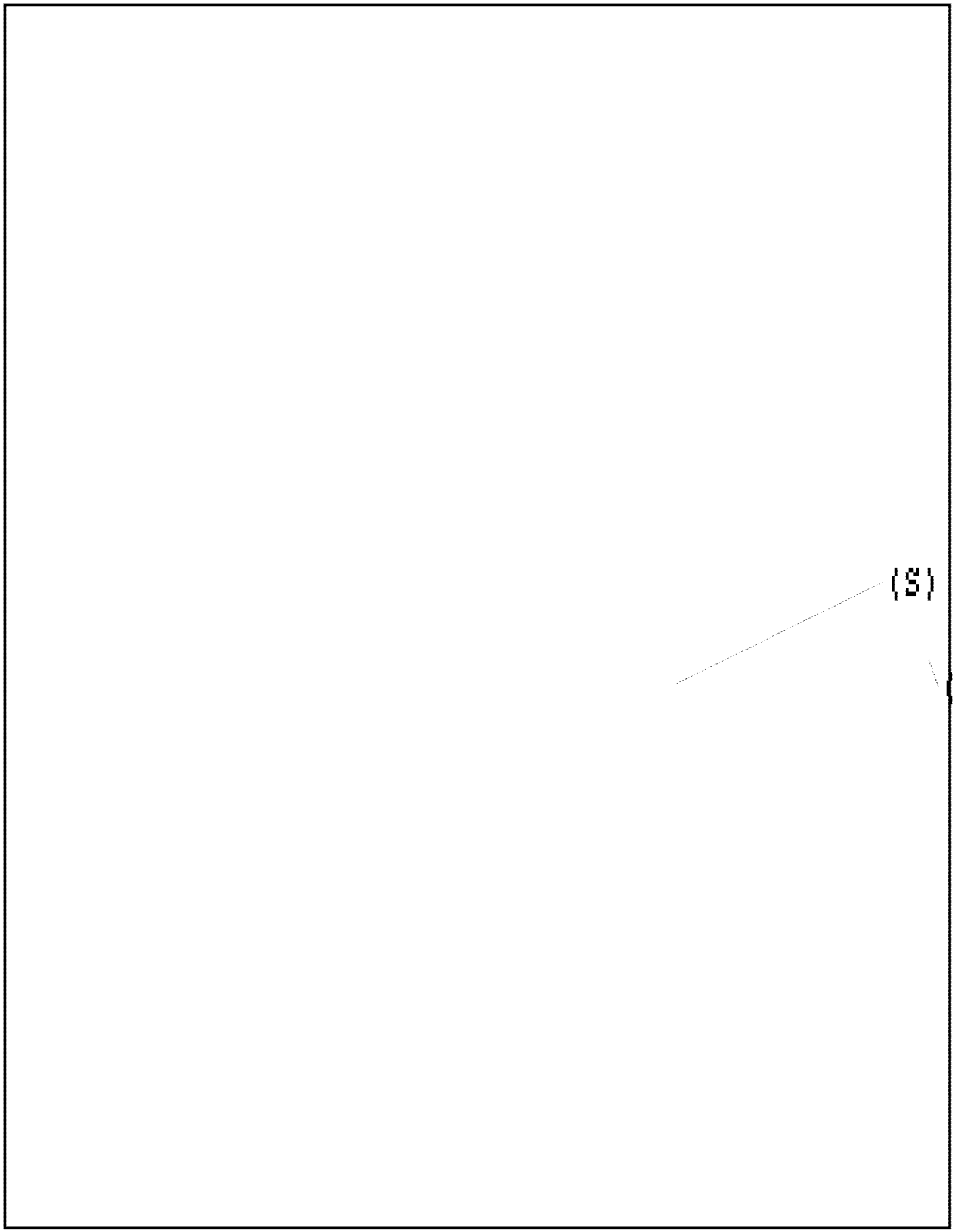
b1
b2
b6
b7A
b7E

(S)

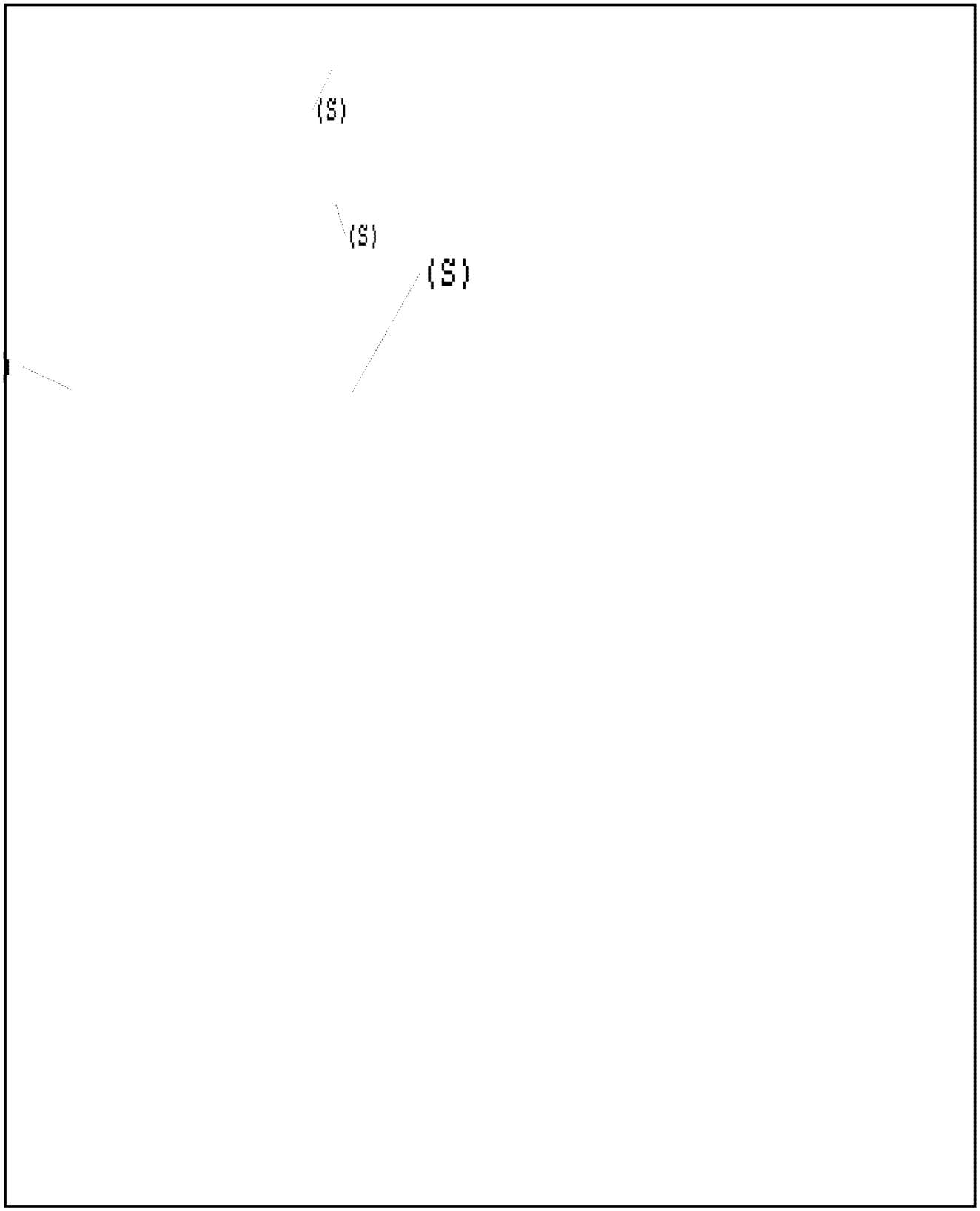


b2
b7E

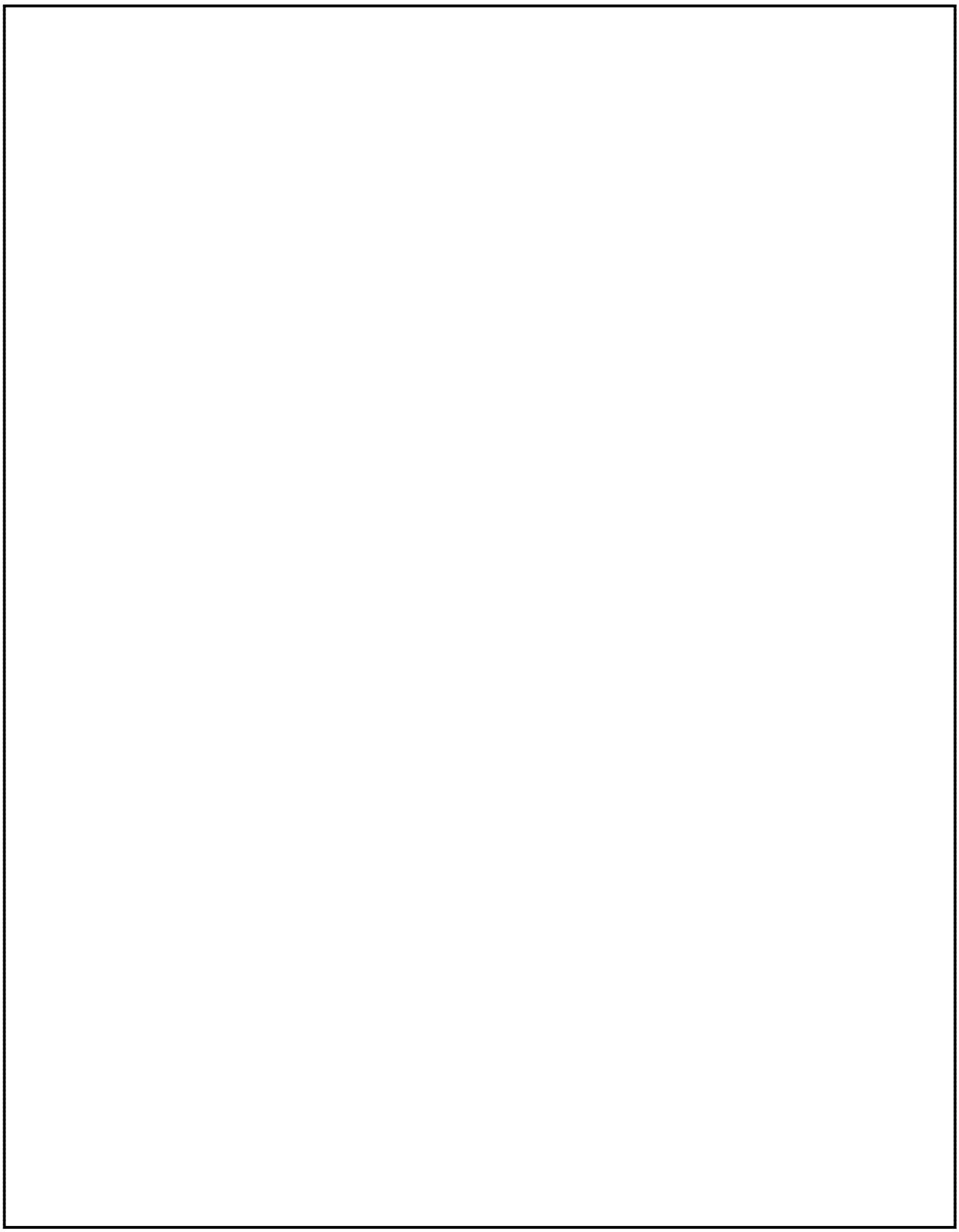
b1
b2
b6
b7A
b7C
b7E



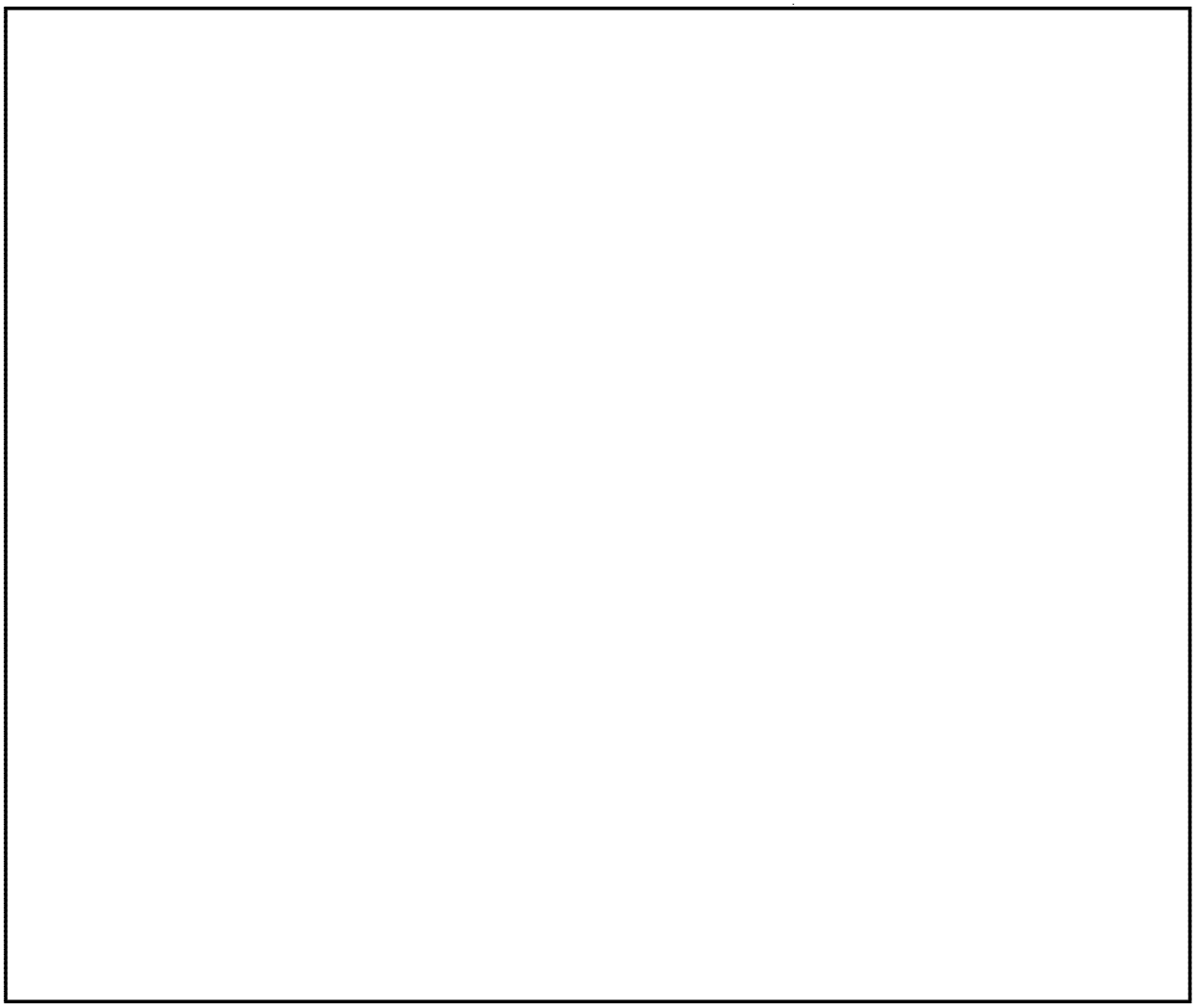
b1
b2
b6
b7A
b7C
b7E



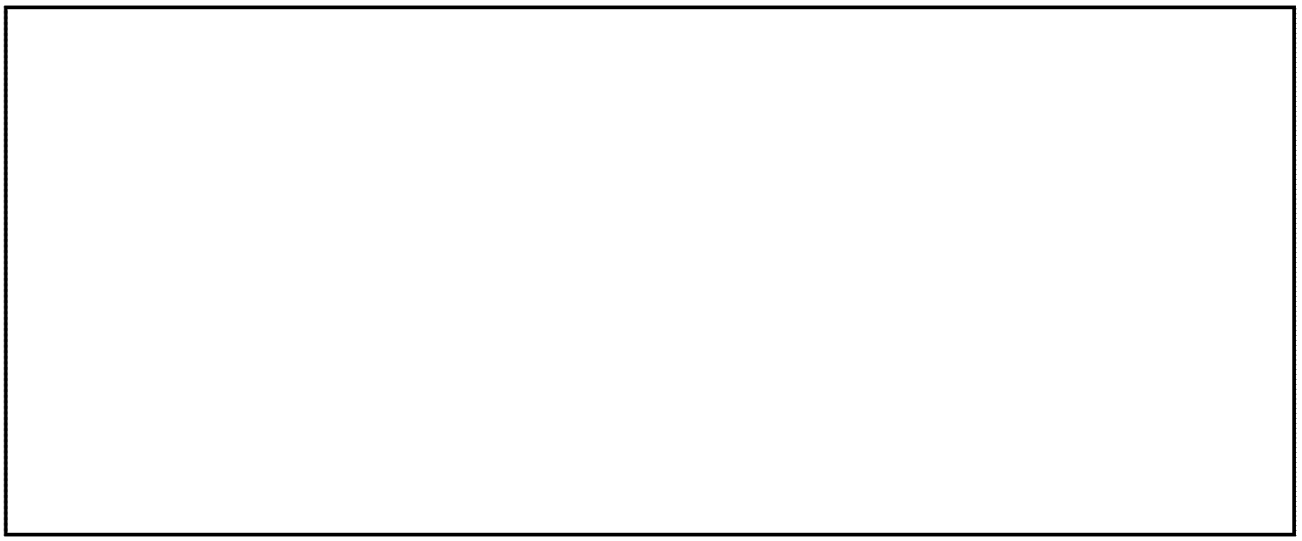
b2
b6
b7A
b7C
b7E



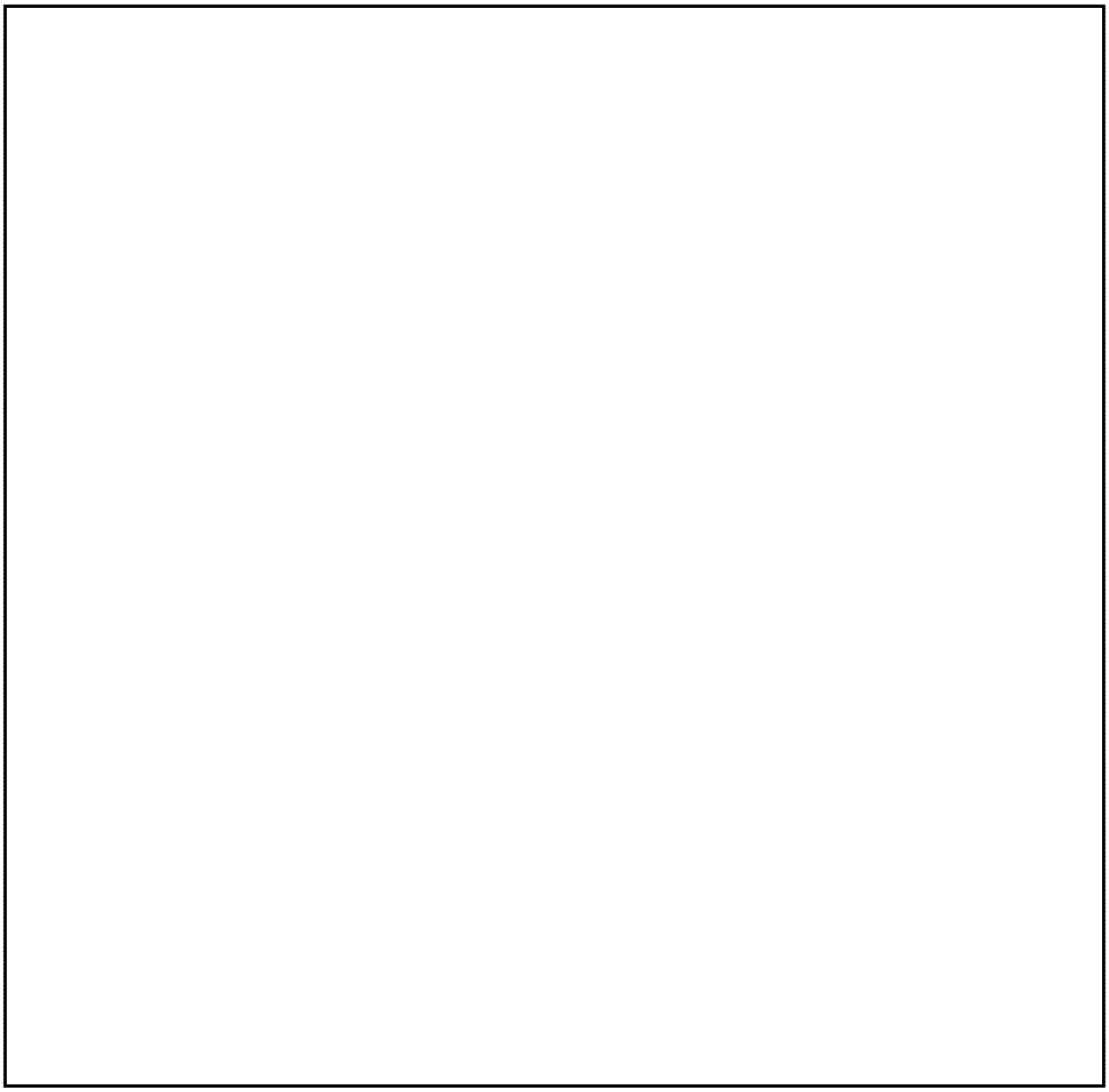
b2
b7E



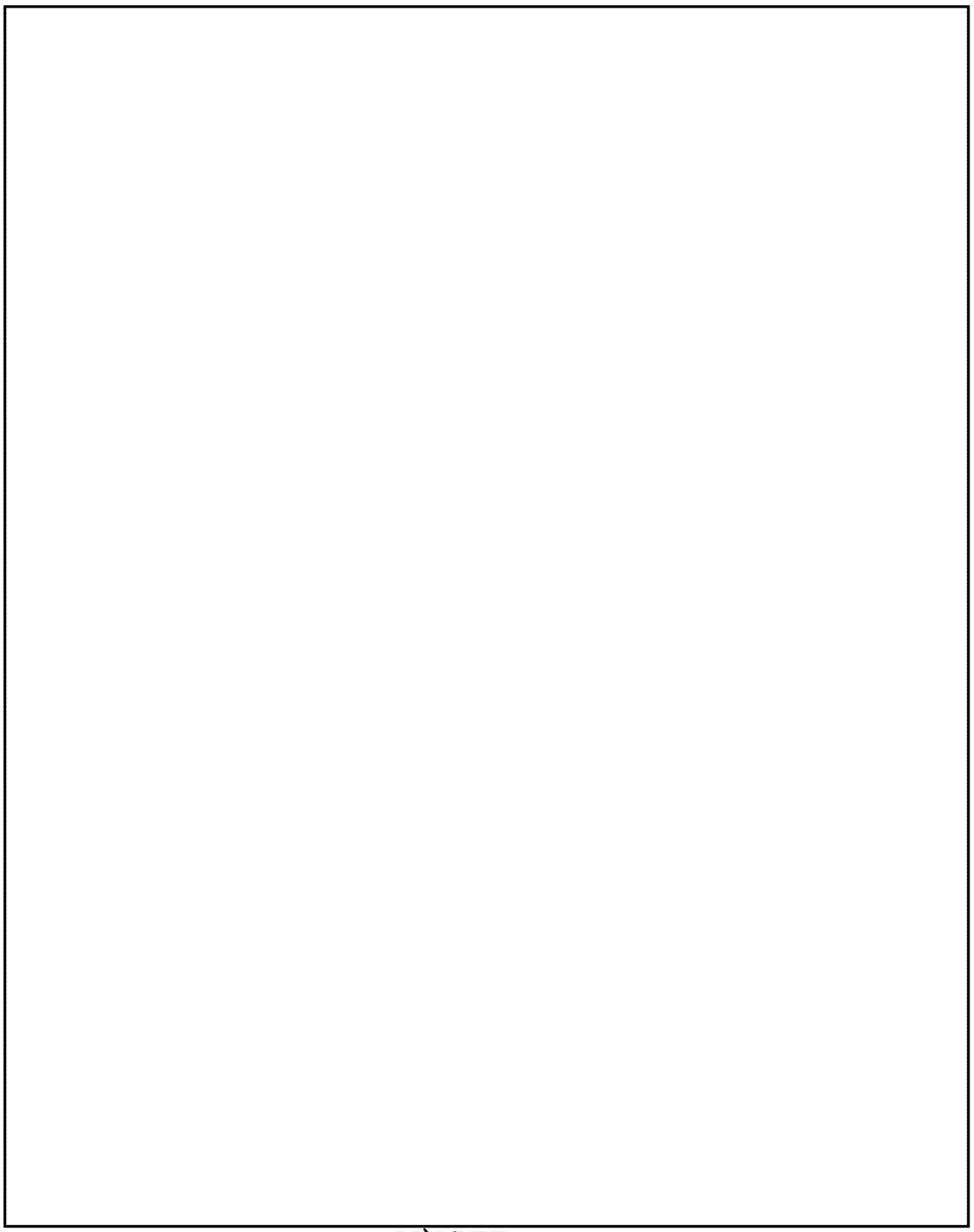
b5



b2
b6
b7A
b7C
b7E



b2
b6
b7A
b7C
b7E



[redacted]

b1
b2
b6
b7A
b7C
b7E

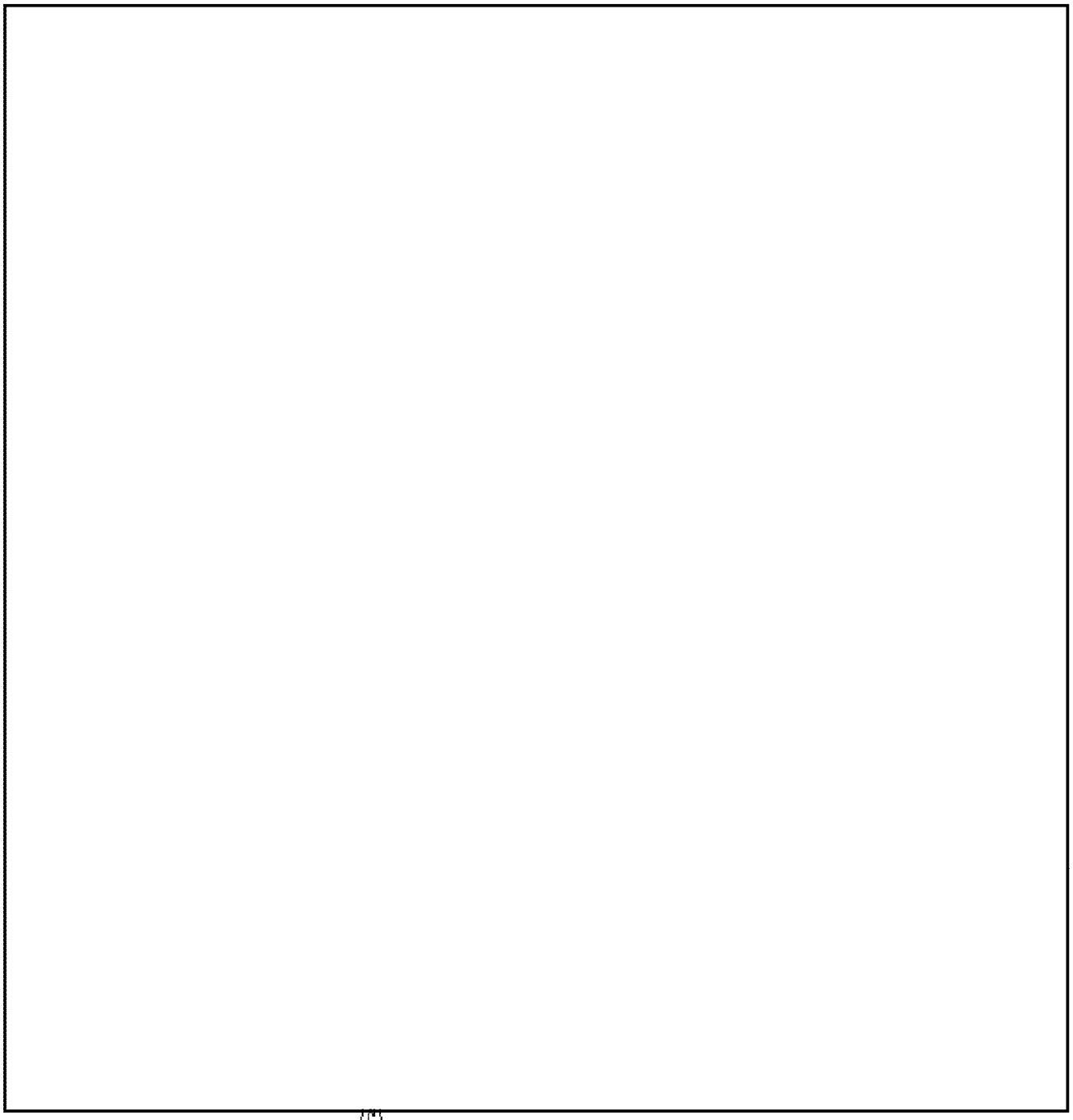
[redacted]

(S)

(S)

[redacted]

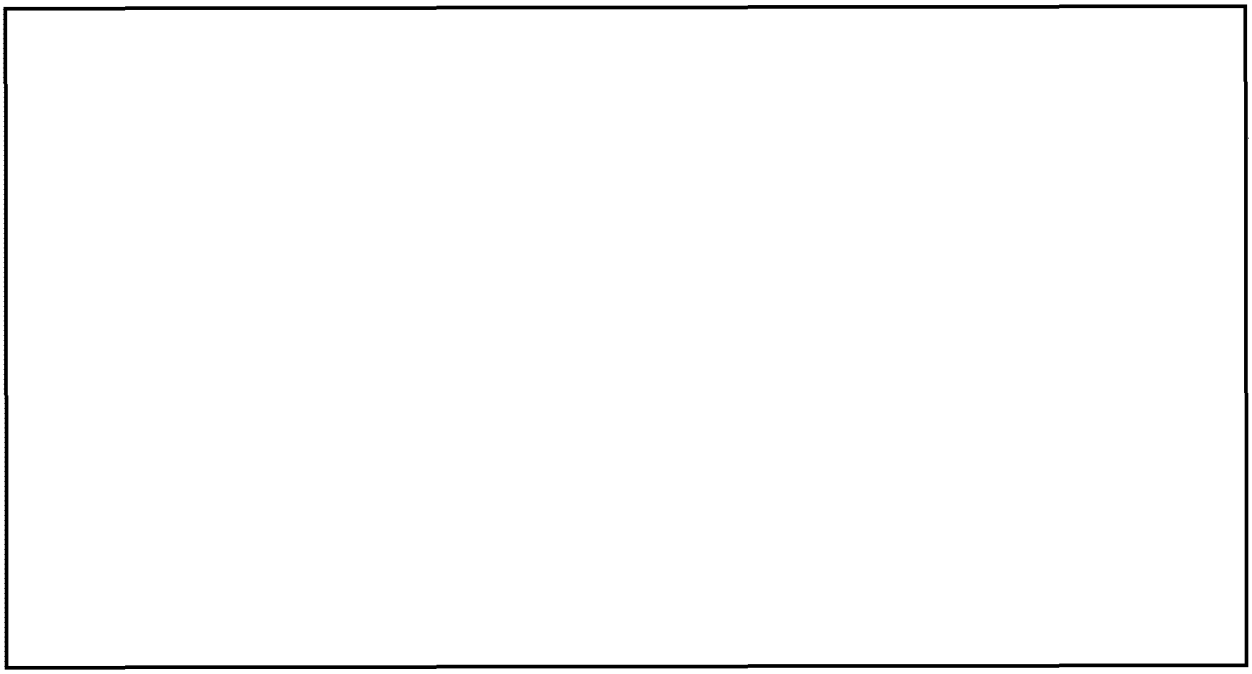
(S)



b1
b2
b6
b7A
b7C
b7D
b7E

(S)

b2
b7E



b2

A. OPERATIONAL EXAMPLES OF USA PATRIOT ACT SUCCESSES (TEAM 1 [redacted] b7E

1. Sharing grand jury, Title III, and criminal investigative information (Sec. 203):

- FBINY obtained U.S. financial records through federal grand jury subpoenas. Information obtained from these records was also shared with the USIC and other terrorism cases were opened based on this intelligence.
- The Patriot Act enabled the FBI and Bureau of Prisons (BOP) to work together, sharing information regarding violations of Special Administrative Methods (SAM), in particular illegal communications between incarcerated terrorists and their attorneys (see Lynne Stewart conviction).

2. "Roving" FISA ELSUR authority:

3. Changes in FISA PR/TT authority (Sec. 214):

4. Changes in FISA business records authority:

b7A

5. Use of Library Records:

- [redacted]

B. ADDITIONAL TOOLS & TWEAKS, i.e., WISH LIST

- One example of a need is an administrative subpoena power related to CTD efforts. We have that authority for Drugs and Health Care fraud matters, why not CT investigations which are just as important?

Patriot Act Successes
ITOS I/CONUS I

Team 1

- FB[ ]btained U.S. financial records through federal grand jury subpoenas. Information obtained from these records was also shared with the USIC and other terrorism cases were opened based on this intelligence. b2 b7E
- The Patriot Act enabled the FBI and Bureau of Prisons (BOP) to work together[ ]
[ ] b2 b7E
- [ ]led to a recent indictment for making a false bomb threat to the government along with numerous 1001 violations. b2 b7E

B. ADDITIONAL TOOLS

- One example of a need is an administrative subpoena power related to CTD efforts. We have that authority for Drugs and Health Care fraud matters, why not CT investigations which are just as important?

Team 2 & 3

[ ]

- **Changes in FISA business records authority:**[ ]
[ ] b2 b7E
- Section 215 of the Patriot Act allows the FBI to seek a FISA court order for any tangible materials such as books, records, papers, documents, and other items.

[ ]

Section 214 Changes in FISA/PR/TT authority:

- **Changes in FISA PR/TT authority:**[ ] b2 b7E
[ ]

b2
b7E

- **Sharing grand jury, Title III, and criminal investigative information.**

Team 4

Section 203 Sharing criminal investigative information:

b2
b7E

- (U)

b2

Section 214 Changes in FISA/PR/TT authority:

b7E

- (U)

Section 215 Changes in FISA business records authority:

- (U)

b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 09-23-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (C, D)
DECLASSIFY ON: 09-23-2030

CONUS 2 PATRIOT ACT EXAMPLES:

1. Subje[redacted] (S)

b6
b7C
b7A

Predication:

[redacted] (S)

b1
b2
b7E
b6
b7C
b7A

Patriot Act usage:

[redacted] (S)

b1
b2
b7E
b7A

[redacted] (S)

b1
b6
b7C
b7A

From: [redacted] (OGC) (FBI)
Sent: Wednesday, March 23, 2005 11:49 AM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (OCA) (FBI)
Subject: FW: Responses for Director's Testimony/Patriot Act

b6
b7C

UNCLASSIFIED
RECORD 315N-SE

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-23-2005 BY 65179 DMH/JHF 05-CV-0845

#3
-----Original Message-----
From: [redacted] (OGC)(FBI)
Sent: Tuesday, March 22, 2005 5:10 PM
To: [redacted] OGC) (FBI)
Subject: FW: Responses for Director's Testimony/Patriot Act

b6
b7C

UNCLASSIFIED
RECORD 315N-SE

-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Friday, March 18, 2005 7:20 PM
To: [redacted] CTD) (FBI)
Cc: [redacted] OGC)(FBI)
Subject: FW: Responses for Director's Testimony/Patriot Act

b6
b7C

UNCLASSIFIED
RECORD 315N-SE

Patriot Act info

[redacted]
CTD/ITOS 1/Conus IV
[redacted]

b6
b7C

b6
b7C

-----Original Message-----
From: [redacted] CTD) (FBI)
Sent: Friday, March 18, 2005 11:15 AM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (CTD) (FBI)
Subject: Responses for Director's Testimony/Patriot Act

b6
b7C

UNCLASSIFIED
RECORD 315N-SE

b6
b7C

[redacted]

[redacted] sked that we provide examples of Patriot Act info/examples from our division's of responsibility, which are being compiled for the director's testimony. This is a [redacted] example of timely criminal investigative/intel info

b2
b7E

b2
b7E

sharing with the Department of Defense (Army):

(U)

Thanks for passing this along.

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

From: (OGC) (FBI)
Sent: Wednesday, March 23, 2005 11:49 AM
To: (CTD) (FBI)
Cc: (OCA) (FBI)
Subject: FW: Bullets for Director's Senate Testimony

b6
b7C

DATE: 09-23-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (C ,D)
DECLASSIFY ON: 09-23-2030

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

#2
-----Original Message-----
From: (OGC)(FBI)
Sent: Tuesday, March 22, 2005 5:09 PM
To: (OGC) (FBI)
Subject: FW: Bullets for Director's Senate Testimony

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

-----Original Message-----
From: CTD) (FBI)
Sent: Monday, March 21, 2005 12:53 PM
To: CTD) (FBI)
Cc: (OGC)(FBI)
Subject: RE: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Thanks. is handling that, I'm not doing anything about the Patriot Act tasking.

b6
b7C

CTD/ITOS-1

b6
b7C

-----Original Message-----
From: (CTD) (FBI)
Sent: Friday, March 18, 2005 7:18 PM
To: (CTD) (FBI)
Cc: (OGC)(FBI)
Subject: FW: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Patriot Act tasking

b6
b7C

SECRET

CTD/ITOS 1/Conus IV

[redacted]

b6
b7C

-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Friday, March 18, 2005 11:01 AM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (CTD) (FBI); [redacted] (CTD) (FBI)
Subject: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

b1

[redacted]

Here is a bullet for the [redacted] division:

b2
b6
b7C
b7E

(S) [redacted]

(S)

Thanks,

[redacted]

IA [redacted]
CTD/ITOS I/CONUS IV

[redacted]

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

SECRET

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

From (OGC) (FBI)
Sent: Wednesday, March 23, 2005 11:49 AM
To TD) (FBI)
Cc (OCA) (FBI)
Subject: FW: Bullets for Director's Senate Testimony

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

DATE: 09-23-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C , D)
DECLASSIFY ON: 09-23-2030

#4
-----Original Message-----
From: (OGC)(FBI)
Sent: Tuesday, March 22, 2005 5:11 PM
To (OGC) (FBI)
Subject: FW: Bullets for Director's Senate Testimony

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

-----Original Message-----
From: CTD) (FBI)
Sent: Friday, March 18, 2005 7:18 PM
To: TD) (FBI)
Cc: OGC)(FBI)
Subject: FW: Bullets for Director's Senate Testimony

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Patriot Act tasking

CTD/ITOS 1/Conus IV

-----Original Message-----
From: (CTD) (FBI)
Sent: Friday, March 18, 2005 11:01 AM SECRET
To (CTD) (FBI)
Cc: (CTD) (FBI); (CTD) (FBI); (CTD) (FBI)
Subject: Bullets for Director's Senate Testimony

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Here is a bullet for the division:

(U)

b6
b7C
b6
b7C
b6
b7C
b2
b7C
b6
b7C
b2 , b7E

[redacted] (S)

b1
b6
b7C
b2
b7E

Thanks,

[redacted]

IA [redacted]
CTD/ITOS I/CONUS IV

b6
b7C

[redacted]

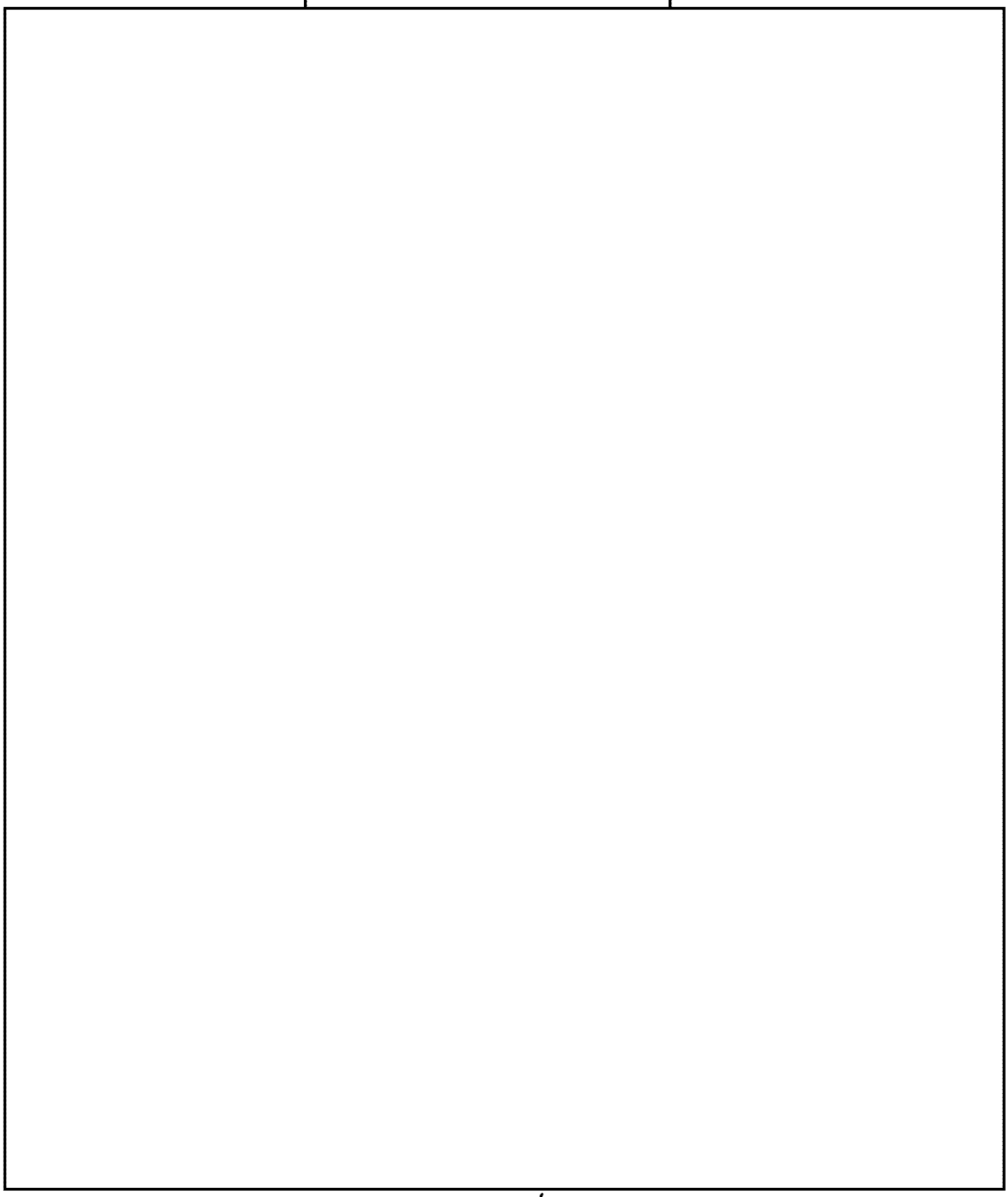
~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

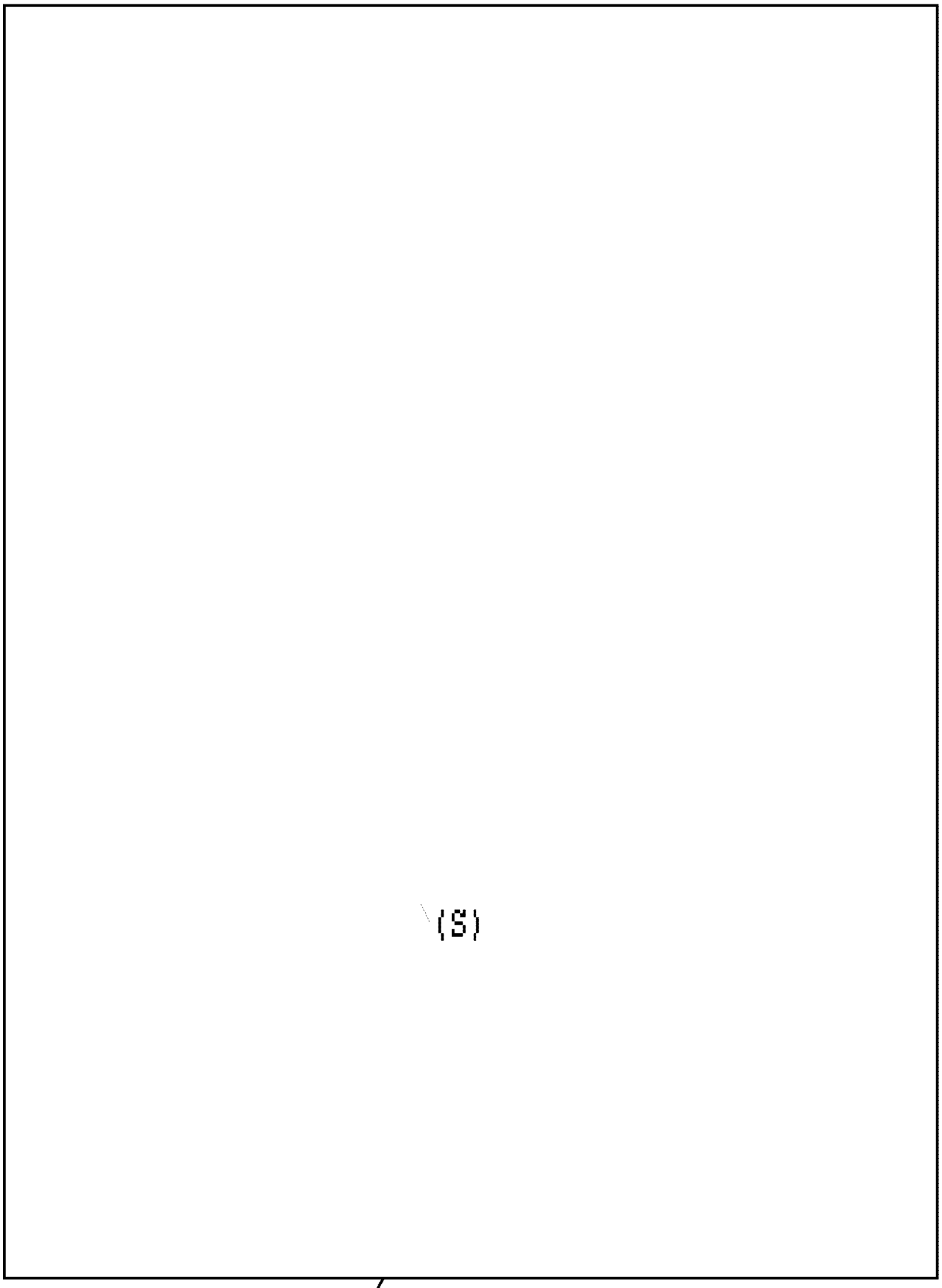
~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

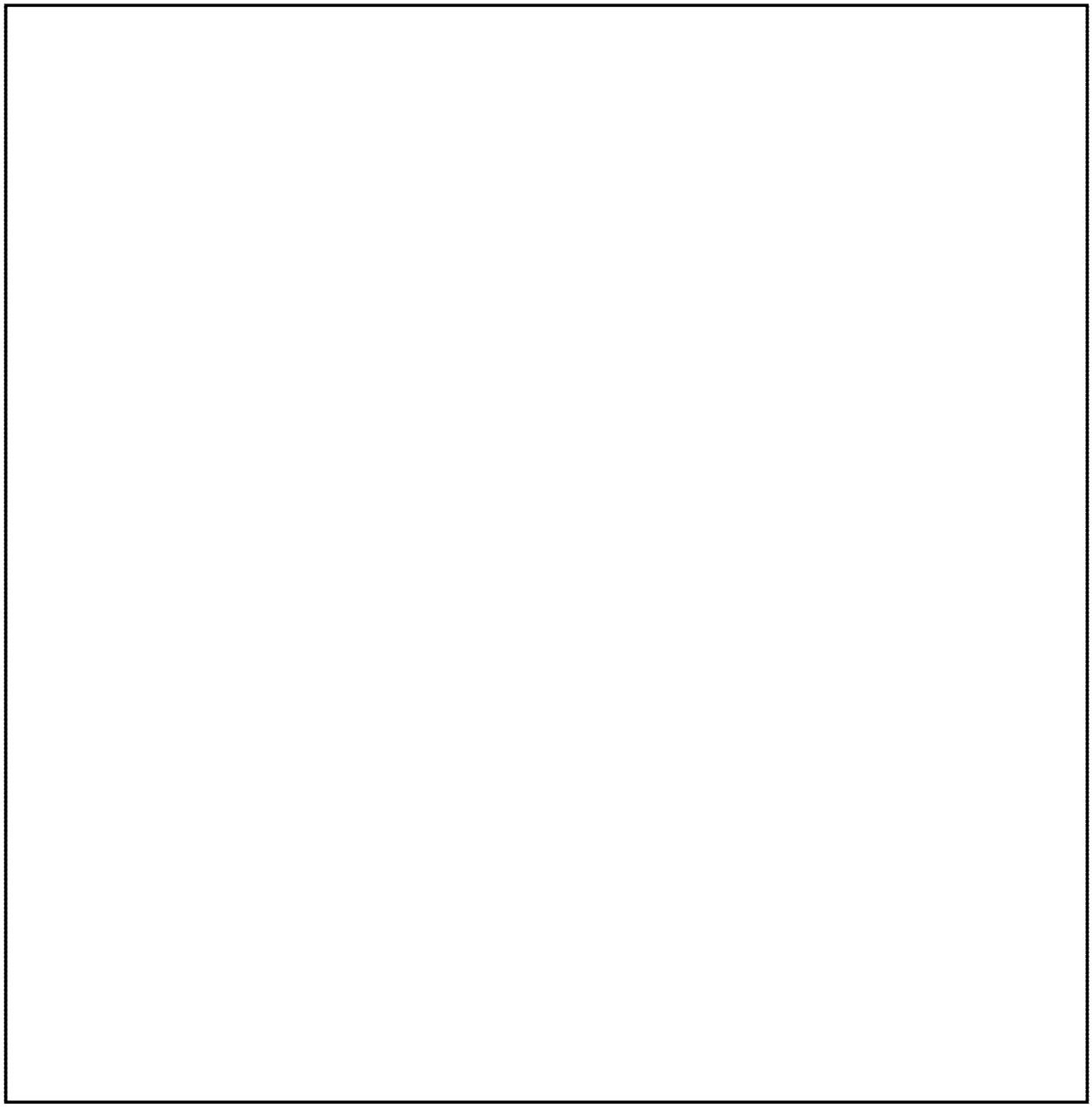
SECRET



b1
b2
b7E



b2
b5
b7E



PATRIOT Act Response
WMD/Domestic Terrorism Operations Section (WMD/DTOS)
FBIHQ
03/23/2005

Item #1
Special Events Management Unit/Civil Aviation Security Program (SEMU/CASP)
FBIHQ POC: SSA [redacted] b6 b7C

The Patriot Act was used by the [redacted] Field Office to charge David Banach with one (1) count of Title 18 Section 1993 (a) 5 (Terrorist attacks and other acts of violence against mass transportation systems with reckless disregard for the safety of human life) On or about January 5, 2005. Mr. Banach was the individual who "lazed" a charter aircraft coming into Teteboro Airport on December 29, 2004. The case is still an active investigation. SA [redacted] in [redacted] is the POC. b2 b7E b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Item #2
Domestic Terrorism Operations Unit (DTOU)
FBIHQ POC: SSA [redacted] b6 b7C

We have had two recent investigations where we identified a victim of a computer intrusion and requested their assistance in monitoring of a computer controlled by the victim. In both cases a denial of service attack occurred using botnets and the Agents were able to identify the victim computer (server) after analyzing computers where the attack occurred. The Agents contacted the victims after determining they were not involved in the criminal act and they agreed to have sniffers attached to their computers. The purpose of this was the subject was using the victim's computer to direct or reprogram the "bots" for additional criminal activity. When the subjects logged onto the victim's computer the Agents could determine where the computer was located and direct the investigation to a new computer. This then only leads us to additional compromised computers and we start the process over to monitor the new computer.

Item #3
Domestic Terrorism Operations Unit (DTOU)
FBIHQ POC: SSA [redacted] b6 b7C

DATE: 09-29-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-29-2030

(S)

I cannot speak for whether the [redacted] were obtained based primarily upon legal changes resulting from the Patriot Act. The [redacted] investigation was conducted during the period that the Patriot Act was evolving. (S) b1 b6 b7C

General Summary:

- [redacted] (S) b1 b2 b7E

- [redacted] (S)
- [redacted]
- [redacted]
- [redacted]
- [redacted]

b1
b6
b7C
b2
b7E

[redacted] (S)

b1
b6
b7C
b2
b7E

[redacted] (S)

b1
b2
b7E
b6
b7C

Item #4
Domestic Terrorism Operations Unit (DTOU)
FBIHQ POC: SSA [redacted]

b6
b7C

Note - I believe you received this already

In response to your e-mail disseminated to the filed, dated 03/17/2005, concerning feedback on the utility of the Patriot Act sunset provisions, [redacted] after canvassing all relevant squads, responds as follows:

b2
b7E

(S) Since the inception of the Patriot Act, the [redacted] JTTF [redacted] (S) [redacted] of use of the Expanded Title III Predicates (sections 201 and 202), Roving Wiretaps (section 206) or Computer Hacking Victims Requesting Law Enforcement Assistance (section 217). All pen registers currently and in the past three years that are being utilized by the [redacted] are being done via criminal justification.

b1
b2
b7E

On November 12, 2004 the Patriot Act (section 215) was used for obtaining a National Security Letter (NSL) on a lead out of Headquarters for case [redacted] In this particular instance, telephone toll records were needed on a Secret classified case and the NSL allowed lead agents to obtain the information without having to obtain a subpoena or reveal the nature of the investigation.

b7A

The most common use of the Patriot Act on the [redacted] is for disseminating information in ACS that is terrorism related to state and local law enforcement (sections 203 and 218). To date, the [redacted] has provided information to the National Security Bureau (NSB) of the [redacted] Metropolitan Police Department on [redacted] occasions. The [redacted] also coordinates information sharing with BICE, the Department of Homeland Security, the US Marshals, DEA, IRS, FAM, Air Force OSI, the US Secret Service, the [redacted] Attorney Generals Office, and [redacted] Police Departments under the same Patriot Act sections (203 and 218).

b2
b7E

The [redacted] Division has been conducting a significant Bribery, Graft and Conflicts of Interest Title 18 U.S.C. Section 201 investigation involving large amounts of money laundering. [redacted] and [redacted] maintained

b2
b7E
b6
b7C

corrupt relationships with [redacted] public officials designed to protect and enhance [redacted] financial interests. Due to the high profile nature of this case and the impact on [redacted] Division requested a USA Patriot Act Section 314 (a) disclosure of all banks with accounts, safe deposit boxes, and other 314(a) regarding our subjects in the case. In consultation with the Division's CDC and the United States Attorney's Office, it was decided that utilization of the Patriot Act provisions relating to money laundering would benefit the investigation. Although some publicity resulted from the requests made of the financial institutions, the resulting information was significant to the investigation. The overall outcome was positive and resulted in similar requests by other divisions to utilize the Patriot Act in non-Terrorism investigations. b6 b7C b2 b7D

We hope this feedback, when coupled with input from other field offices, will aid in our preservation of the essential sunset provisions of the Patriot Act.

Item #5
Domestic Terrorism Operations Unit (DTOU)
FBIHQ POC: SSA [redacted] b6 b7C

174A-OC-66039

[redacted] Comm Center received a bomb threat at 3:00 a.m. on 8/5/04. After clarifying that the bomb threat was to the local airport and that the FBI had until noon to meet the caller's demands, JTTF agents began tracing the caller id. Investigation showed the Internet was used to make the call via VoIP. The VoIP service provider provided the IP address along with the date and time of registration of the individual who was responsible for making the threat. To obtain the subscriber info to identify the individual, an emergency disclosure, as per the Patriot Act, was instituted with Comcast, the ISP used by the individual. By 7:00 a.m., a subject in [redacted] was identified. [redacted] division conducted a subject interview and the threat was determined to be non-credible by 11:00 a.m. b2 b7E

Testimony of Robert S. Mueller, III

Director, Federal Bureau of Investigation

Before the United States Senate

Committee on the Judiciary

May 20, 2004

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to be here today to update you on the FBI's substantial progress in the counterterrorism and intelligence arenas since my last appearance before the Committee. I would also like to acknowledge that the progress the FBI has made in reforming our counterterrorism and intelligence programs is due in no small part to the enactment of the USA PATRIOT Act.

Every day, the men and women of the FBI demonstrate their determination to fulfill the great responsibility that you, and the public, have entrusted to them. As a result, the FBI has made steady progress in meeting our highest priority of preventing terrorism. The terrorist threat presents complex challenges. Terrorists move easily across international borders, use sophisticated technology to recruit, network, and communicate, and finance their operations with elaborate funding schemes. Above all, they are patient. They are methodical. They are determined to succeed.

But the FBI is equally determined to succeed. To defeat these threats, the FBI must have several critical capabilities: First, we must develop intelligence about terrorist activity and use that intelligence to disrupt their plans. Second, we must be global – we must work closely with our counterparts at home and abroad to develop and pool our collective knowledge and expertise. Third, we must use cutting-edge information technology to collect, analyze, manage, and share our information effectively. Most importantly, we must work within the framework of the Constitution, protecting our cherished civil liberties as we work to protect the American people.

Today, I would like to give you a brief overview of the steps we have taken to put these critical capabilities in place by reforming our counterterrorism and intelligence programs, as well as overhauling our information technology. Before I begin, however, I would like to acknowledge that none of our successes would have been possible without the extraordinary efforts of our partners in state and municipal law enforcement and our counterparts around the world. The Muslim, Iraqi, and Arab-American communities have also contributed a great deal to the war on terror. On behalf of the FBI, I would like to thank these communities for their assistance and for their ongoing commitment to preventing acts of terrorism. The country owes them a debt of gratitude.

PATRIOT ACT

Mr. Chairman, for over two and a half years, the PATRIOT Act has proved extraordinarily beneficial in the war on terrorism and has changed the way the FBI does business. Many of our counterterrorism successes, in fact, are the direct results of provisions included in the Act, a number of which are scheduled to "sunset" at the end of next year. I strongly believe it is vital to our national security to keep each of these provisions intact. Without them, the FBI could be forced back into pre-September 11 practices, attempting to fight the war on terrorism with one hand tied behind our backs.

Let me give you just a few examples that illustrate the importance of the PATRIOT Act to our counterterrorism efforts:

First and foremost, the PATRIOT Act – along with the revision of the Attorney General's investigative guidelines and the 2002 decision of the Foreign Intelligence Surveillance Court of Review – tore down the wall that stood between the intelligence investigators responding to terrorist threats and the criminal investigators responding to those same threats.

• Prior to September 11, an Agent investigating the intelligence side of a terrorism case was barred from discussing the case with an Agent across the hall who was working the criminal side of that same investigation. For instance, if a court-ordered criminal wiretap turned up intelligence information, the criminal investigator could not share that information with the intelligence investigator – he could not even suggest that the intelligence investigator should seek a wiretap to collect the information for himself. If the criminal investigator served a grand jury subpoena to a suspect's bank, he could not divulge any information found in those bank records to the intelligence investigator. Instead, the intelligence investigator would have to issue a National Security Letter in order to procure that same information.

• The removal of the "wall" has allowed government investigators to share information freely. Now, criminal investigative information that contains foreign intelligence or counterintelligence, including grand jury and wiretap information, can be shared with intelligence officials. This increased ability to share information has disrupted terrorist operations in their early stages -- such as the successful dismantling of the "Portland Seven" terror cell -- and has led to numerous arrests, prosecutions, and convictions in terrorism cases.

• In essence, prior to September 11th, criminal and intelligence investigators were attempting to put together a complex jigsaw puzzle at separate tables. The Patriot Act has fundamentally changed the way we do business. Today, those investigators sit at the same table and work together on one team. They share leads. They fuse information. Instead of conducting parallel investigations, they are fully integrated into one joint investigation.

• Because of the creation of the Terrorist Threat Integration Center, and because the FBI has dramatically improved its information sharing with the CIA, the NSA, and a host of other federal, state, local and international partners, our resources are used more effectively, our investigations are conducted more efficiently, and America is immeasurably safer as a result. We cannot afford to go back to the days when Agents and prosecutors were afraid to share information.

Second, the PATRIOT Act gave federal judges the authority to issue search warrants that are valid outside the issuing judge's district in terrorism investigations. In the past, a court could only issue a search warrant for premises within the same judicial district – yet our investigations of terrorist networks often span multiple districts. The PATRIOT Act streamlined this process, making it possible for judges in districts where activities related to terrorism may have occurred to issue search warrants applicable outside their immediate districts.

In addition, the PATRIOT Act permits similar search warrants for electronic evidence such as email. In the past, for example, if an Agent in one district needed to obtain a search warrant for a subject's email account, but the Internet service provider (ISP) was located in another district, he or she would have to contact an AUSA and Agent in the second district, brief them on the details of the investigation, and ask them to appear before a judge to obtain a search warrant – simply because the ISP was physically based in another district. Thanks to the PATRIOT Act, this frustrating and time-consuming process can be averted without reducing judicial oversight. Today, a judge anywhere in the U.S. can issue a search warrant for a subject's email, no matter where the ISP is based.

Third, the PATRIOT Act updated the law to match current technology, so that we no longer have to fight a 21st-century battle with antiquated weapons. Terrorists exploit modern technology such as the Internet and cell phones to conduct and conceal their activities. The PATRIOT Act leveled the playing field, allowing investigators to adapt to modern techniques. For example, the PATRIOT Act clarified our ability to use court-ordered pen registers and trap-and-trace devices to track Internet communications. The Act also enabled us to seek court-approved roving wiretaps, which allow investigators to conduct electronic surveillance on a particular suspect, not a particular telephone – this allows them to continuously monitor subjects without having to return to the court repeatedly for additional authorizations. This technique has long been used to investigate crimes such as drug trafficking and racketeering. In a world in which it is standard operating procedure for terrorists to rapidly change locations and switch cell phones to evade surveillance, terrorism investigators must have access to the same tools.

In a final example, the PATRIOT Act expanded our ability to pursue those who provide material support or resources to terrorist organizations. Terrorist networks rely on individuals for fund-raising, procurement of weapons and explosives, training, logistics, and recruiting. The material support statutes allow investigators to aggressively pursue and dismantle the entire terrorist network, from the financiers to those who carry out terrorist plans. By criminalizing the actions of those who provide, channel, or direct resources to terrorists, the material support statutes provide an effective tool to intervene at the earliest possible stage of terrorist planning. This allows the FBI to arrest terrorists and their supporters before their deadly plans can be carried out.

For instance, the FBI investigated a case in Charlotte, North Carolina, in which a group of Lebanese nationals purchased mass quantities of cigarettes in North Carolina and shipped them to Michigan for resale. Their scheme was highly profitable due to the cigarette tax disparity between the two states. The proceeds of their smuggling were used to fund Hezbollah affiliates and operatives in Lebanon. Similarly, the FBI investigated a case in San Diego in which subjects allegedly negotiated with undercover law enforcement officials the sale of heroin and hashish in exchange for Stinger anti-aircraft missiles, which they indicated were to be sold to Al Qaida. In both cases, the material support provisions allowed prosecutors to charge the subjects and secure guilty pleas and convictions.

Mr. Chairman and Members of the Committee, the importance of the PATRIOT Act as a valuable tool in the war against terrorism cannot be overstated. It is critical to our present and future success. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect innocent lives, while at the same time protecting civil liberties.

COUNTERTERRORISM AND INTELLIGENCE PROGRAM REFORMS

Let me turn for a few moments to the progress the FBI has made in strengthening and reforming its counterterrorism and intelligence programs to support its number one goal of terrorism prevention. Today, the FBI is taking full advantage of our dual role as both a law enforcement and an intelligence agency. Let me give you just a few examples of the progress we have made:

• We have more than doubled the number of counterterrorism Agents, intelligence analysts, and linguists.

• We expanded the Terrorism Financing Operations Section, which is dedicated to identifying, tracking, and cutting off terrorist funds.

• We are active participants in the Terrorist Threat Integration Center and the Terrorist Screening Center, which provides a new line of defense against terrorism by making information about known or suspected terrorists available to federal, state, and local law enforcement.

• We have worked hard to break down the walls that have sometimes hampered our coordination with our partners in federal, state and local law enforcement. Today, the FBI and CIA are integrated at virtually every level of our operations. This cooperation will be further enhanced when our Counterterrorism Division co-locates with the CIA's Counter Terrorist Center and the multi-agency Terrorist Threat Integration Center.

• We expanded the number of Joint Terrorism Task Forces (JTTF) from 34 to 84 nationwide.

• We created and refined new information sharing systems, such as the National Alert System, that electronically link us with our domestic partners.

• We have sent approximately 275 FBI executives to the Kellogg School of Management at Northwestern University to receive training on executive leadership and strategic change.

Recognizing that a strong, enterprise-wide intelligence program is critical to our success across all investigations, we have worked relentlessly to develop a strong intelligence capability and to integrate intelligence into every investigation and operation across the FBI:

• We stood up the Office of Intelligence, under the direction of a new Executive Assistant Director for Intelligence. The Office of Intelligence sets unified standards, policies, and training for analysts, who examine intelligence and ensure it is shared with our law enforcement and intelligence partners. The Office of Intelligence has already provided over 2,600 intelligence reports and other documents for the President and members of the Intelligence Community.

• We established a formal analyst training program. We are accelerating the hiring and training of analytical personnel, and developing career paths for analysts that are commensurate with their importance to the mission of the FBI.

• We developed and are in the process of executing Concepts of Operations governing all aspects of the intelligence process – from the identification of intelligence requirements to the methodology for intelligence assessment to the drafting and formatting of intelligence products.

• We established a Requirements and Collection Management Unit to identify intelligence gaps and develop collection strategies to fill those gaps.

• We established Reports Officers positions and Field Intelligence Groups in the field offices, whose members review investigative information – not only for use in investigations in that field office – but to disseminate it throughout the FBI and among our law enforcement and Intelligence Community partners.

With these changes in place, the Intelligence Program is established and growing. We are now turning to the last structural step in our effort to build an intelligence capacity. In March, I authorized new procedures governing the recruitment, training, career paths and evaluation of our Special Agents – all of which are focused on developing intelligence expertise among our agent population.

The most far-reaching of these changes will be the new agent career path, which will guarantee that agents get experience in intelligence investigations and with intelligence processes. Under this plan, new agents will spend an initial period familiarizing themselves with all aspects of the Bureau, including intelligence collection and analysis, and then go on to specialize in counterterrorism, intelligence or another operational program. A central part of this initiative will be an Intelligence Officer Certification program that will be available to both analysts and agents.

That program will be modeled after – and have the same training and experience requirements as – the existing programs in the Intelligence Community.

INFORMATION TECHNOLOGY IMPROVEMENTS

All the progress the FBI has made on all investigative fronts rests upon a strong foundation of information technology. Over the past two and a half years, the FBI has made tremendous efforts to overhaul our information technology, and we have made significant progress.

• Over 1,000 counterterrorism and counterintelligence FBI Headquarters employees have been provided with access to Top Secret/Sensitive Compartmented Information (TS/SCI) information at their desks.
• We implemented the Wide Area Network and the Enterprise Operations Center on schedule in March 2003.

• We improved data warehousing technology to dramatically reduce stove-piping and cut down on man-hours that used to be devoted to manual searches.

• The Full Site Capability deployment began in February of this year, and was completed on April 29th. Altogether, nearly 30,000 workstations have been converted to the new Trilogy baseline software and new email system.

• We now have a permanent Chief Information Officer and Chief Technology Officer, who oversee the development and management of all IT projects and systems throughout the FBI. It is important to keep in mind that Trilogy is not the FBI's sole IT system – the FBI has over 200 IT systems, all of which must be maintained, enhanced when necessary, and certified and accredited for security.

As you know, during the past year we have encountered some setbacks regarding the deployment of Trilogy's Full Site Capability (FSC) and the Virtual Case File. Our goal is to deliver Virtual Case File capabilities by the end of this year. You are aware that last week, the National Research Council of the National Academies (NRC) released a report reviewing the Trilogy IT Modernization program. The FBI commissioned this review as part of our ongoing efforts to improve our capabilities to assemble, analyze and disseminate investigative and operational data both internally and externally with other intelligence and law enforcement agencies.

Many of the NRC's recommendations have already been implemented or are a work in progress. The FBI has repeatedly sought outside evaluation and advice throughout its IT modernization efforts and will continue to do so. The NRC report specifically noted that the counterterrorism mission requires extensive information sharing, and recommended that the FBI involve other agencies in its modernization program. We will continue to work closely with other Department of Justice Agencies and members of the Homeland Security and Intelligence Communities to ensure the FBI has the right technology to support information sharing and other mission requirements.

CONCLUSION

With our counterterrorism, intelligence, and information technology initiatives firmly in place, the FBI is moving steadily forward, always looking for ways to evolve and improve so that we remain a step ahead of our enemies. We are looking at ways to assess and adjust our resource needs based on threats, in order to ensure that we have the personnel and resources to meet and defeat all threats.

Mr. Chairman, I would like to commend the men and women of the FBI for their hard work and dedication – dedication both to defeating terrorism and to upholding the Constitution. They have embraced and implemented the counterterrorism and intelligence reforms I have outlined for you today and they are committed to upholding their duty to protect the citizens of the United States.

Mr. Chairman, thank you again for the Committee's support of the FBI and for the opportunity to be here this morning.

I would be happy to answer any questions you might have.

b2
b6
b7A
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 113
Page 110 ~ Duplicate
Page 111 ~ Duplicate
Page 112 ~ Duplicate
Page 113 ~ Duplicate
Page 115 ~ Referral/Direct
Page 116 ~ Referral/Direct
Page 117 ~ Referral/Direct
Page 118 ~ Referral/Direct
Page 119 ~ Referral/Direct
Page 120 ~ Referral/Direct
Page 121 ~ Referral/Direct
Page 122 ~ Referral/Direct
Page 123 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 128 ~ Referral/Direct
Page 129 ~ Referral/Direct
Page 130 ~ Referral/Direct
Page 131 ~ Referral/Direct
Page 132 ~ Referral/Direct
Page 133 ~ Referral/Direct
Page 134 ~ Referral/Direct
Page 135 ~ Referral/Direct
Page 136 ~ Referral/Direct
Page 137 ~ Referral/Direct
Page 138 ~ Referral/Direct
Page 139 ~ Referral/Direct
Page 140 ~ Referral/Direct
Page 141 ~ Referral/Direct
Page 142 ~ Referral/Direct
Page 143 ~ Referral/Direct
Page 144 ~ Referral/Direct
Page 145 ~ Referral/Direct
Page 146 ~ Referral/Direct
Page 147 ~ Referral/Direct
Page 148 ~ Referral/Direct
Page 262 ~ Referral/Direct
Page 263 ~ Referral/Direct
Page 264 ~ Referral/Direct
Page 265 ~ Referral/Direct
Page 266 ~ Referral/Direct
Page 267 ~ Referral/Direct

Page 268 ~ Referral/Direct
Page 269 ~ Referral/Direct
Page 270 ~ Referral/Direct
Page 271 ~ Referral/Direct
Page 272 ~ Referral/Direct
Page 273 ~ Referral/Direct
Page 274 ~ Referral/Direct
Page 275 ~ Referral/Direct
Page 276 ~ Referral/Direct
Page 277 ~ Referral/Direct
Page 278 ~ Referral/Direct
Page 279 ~ Referral/Direct
Page 280 ~ Referral/Direct
Page 281 ~ Referral/Direct
Page 282 ~ Referral/Direct
Page 283 ~ Referral/Direct
Page 284 ~ Referral/Direct
Page 285 ~ Referral/Direct
Page 286 ~ Referral/Direct
Page 287 ~ Referral/Direct
Page 288 ~ Referral/Direct
Page 289 ~ Referral/Direct
Page 290 ~ Referral/Direct
Page 291 ~ Referral/Direct
Page 292 ~ Referral/Direct
Page 293 ~ Referral/Direct
Page 294 ~ Referral/Direct
Page 295 ~ Referral/Direct
Page 296 ~ Referral/Direct
Page 297 ~ Referral/Direct
Page 298 ~ Referral/Direct
Page 299 ~ Referral/Direct
Page 321 ~ Referral/Direct
Page 322 ~ Referral/Direct
Page 323 ~ Referral/Direct
Page 324 ~ Referral/Direct
Page 325 ~ Referral/Direct
Page 326 ~ Referral/Direct
Page 327 ~ Referral/Direct
Page 328 ~ Referral/Direct
Page 329 ~ Referral/Direct
Page 330 ~ Referral/Direct
Page 331 ~ Referral/Direct
Page 332 ~ Referral/Direct
Page 333 ~ Referral/Direct
Page 334 ~ Referral/Direct
Page 335 ~ Referral/Direct
Page 336 ~ Referral/Direct
Page 337 ~ Referral/Direct
Page 338 ~ Referral/Direct
Page 339 ~ Referral/Direct

Page 340 ~ Referral/Direct
Page 341 ~ Referral/Direct
Page 342 ~ Referral/Direct
Page 343 ~ Referral/Direct
Page 344 ~ Referral/Direct
Page 345 ~ Referral/Direct
Page 346 ~ Referral/Direct
Page 347 ~ Referral/Direct
Page 348 ~ Referral/Direct
Page 349 ~ Referral/Direct
Page 350 ~ Referral/Direct
Page 351 ~ Referral/Direct
Page 352 ~ Referral/Direct
Page 353 ~ Referral/Direct
Page 354 ~ Referral/Direct
Page 355 ~ Referral/Direct
Page 356 ~ Referral/Direct
Page 357 ~ Referral/Direct

Sunset Provisions

- On December 31, 2005, sixteen provisions of the USA PATRIOT Act are scheduled to expire. The majority of the provisions scheduled to sunset provide the FBI with investigative tools that were not available prior to September 11th and that have been critical to our success in protecting the American people. While some of the "sunset" provisions have been quite controversial, others have been subject to little criticism.

- We anticipate a spirited debate as Congress, the Executive Branch and the American people evaluate the renewal of these provisions. We are already aware of several hearings in both the House and the Senate on the various provisions. Whether FBI witnesses are testifying or we are supporting Department of Justice witnesses, we will look to the field offices to provide us with examples of how these provisions have assisted in our investigative efforts, with a particular emphasis on our efforts in the war on terror.

- I'd like to focus on the impact of the Patriot Act in a couple of key areas:

[redacted] b5

- Please send examples of success that can be attributed to Patriot Act tools to [redacted] of the Investigative Law Unit, Office of the General Counsel and to [redacted] Office of Congressional Affairs. These individuals may also contact you to respond to specific taskings.

b6
b7C

From: [redacted] (OCA) (FBI)
Sent: Friday, February 11, 2005 1:55 PM
To: [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (LV) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); KALISCH, ELENI P. (OCA) (FBI); [redacted] (OCA)(FBI); [redacted] (OCA) (FBI); [redacted] (KC) (FBI); [redacted] (CTD) (FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI)
Subject: Reauthorization of the USA Patriot Act

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-13-2005 BY 65179 DMH/JHF 05-CV-0845

UNCLASSIFIED
NON-RECORD

During the 109th Congress, the Hill will be considering reauthorization of the USA Patriot Act. There are several specific provisions that will sunset unless renewed by 12/2005. In addition, there are some controversial provisions that are not scheduled to sunset, but that will be the subject of considerable debate. In anticipation of this activity, DOJ OLA has put together a USA Patriot Act working group. DOJ OLA will be closely coordinating activity through the members of the working group - I am representing FBI OCA and [redacted] is participating as a representative of FBI OGC. A couple of items of guidance are offered after the group's first meeting:

b6
b7C

1. AAG Will Moschella announced that DOJ components (including the FBI) are NOT to respond directly to any CONGRESSIONAL CORRESPONDENCE (Member, Constituent and Committee) concerning the USA Patriot Act or any of its provisions. All matters should be referred to DOJ's ExecSec. I've provided guidance to FBI ExecSec. If you receive any incoming correspondence, please forward to the FBI ExecSec for tracking and referral to DOJ. In the case of written inquiries from key members or our oversight committees, we may need to send an interim response upon referring the matter to DOJ. I will work with ExecSec if we determine interim responses are necessary.

2. DOJ OLA will be coordinating all requests for briefings or hearings on Patriot Act. [redacted] is the OLA POC if you get a request for a Patriot Act briefing or identification of a hearing witness. Please 'cc me on any e-mail to [redacted] referring a request for a briefing or hearing witness.

b6
b7C

3. Any other requests for information concerning the Patriot Act should likewise be referred to [redacted] DOJ OLA. (ie telephonic requests for comment on proposed revisions or requests for info (ie case examples) re FBI use of Patriot Act tools) Please 'cc me when referring to DOJ OLA.

b6
b7C

4. DOJ has prepared a binder of briefing material - comprised mostly of material taken from its webpage or www.lifeandliberty.com. I've provided each liaison unit chief with a copy of the binder. There is also an electronic copy of this material on the shared drive (S:/OPCA/OCA/OCAFO/Briefing Material/DOJ Patriot Act Slide Show) Click on the "start.bat" file to activate the show. This material is appropriate for dissemination to Hill staff or field office points of contact in response to general inquiries. DOJ anticipates developing additional briefing material. I will disseminate this additional material as soon as we have it.

DOJ optimistically predicts that Patriot Act reauthorization activity will begin after Easter and conclude in time for the August recess! Please reach out if you have any questions. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

From: [redacted] (RMD) (FBI)
Sent: Monday, February 14, 2005 7:53 AM
To: [redacted] (OCA) (FBI); [redacted] (RMD) (FBI); [redacted] (RMD) (FBI)
Cc: KALISCH, ELENI P. (OCA) (FBI); [redacted] (OCA) (FBI)
Subject: RE: Correspondence re Patriot Act

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-14-2005 BY 65179 DMH/JHF 05-CV-0845

UNCLASSIFIED
NON-RECORD

I will inform my staff. I haven't seen any correspondence lately re: the Patriot Act, but I will let you know if I come across anything.

[redacted]--Please take note of these instructions regarding future correspondence about the Patriot Act and inform your teams.

[redacted]

b6
b7C

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Friday, February 11, 2005 12:58 PM
To: [redacted] (RMD) (FBI); ExecSec (RMD)
Cc: KALISCH, ELENI P. (OCA) (FBI); [redacted] (OCA) (FBI)
Subject: Correspondence re Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted]- during the 109th Congress, the Hill will be considering reauthorization of the USA Patriot Act. It is likely that congressional interest and activity will create general public interest in this topic as well. DOJ has put together a USA Patriot Act working group. At the group's first meeting yesterday, AAG Will Moschella, DOJ Office of Legislative Affairs (OLA), announced that DOJ components (including the FBI) are NOT to respond directly to any CONGRESSIONAL CORRESPONDENCE (Member, Constituent and Committee) concerning the USA Patriot Act or any of its provisions. All matters should be referred to DOJ's ExecSec.

AD Kalisch concurs with this directive from DOJ OLA. However, in the case of written inquiries from key members or our oversight committees, we may need to send an interim response upon referring the matter to DOJ.

Please coordinate with me on these matters. I don't recall seeing any congressional correspondence concerning the Patriot Act recently - please advise if we do have any pending / assigned responses. As we begin to receive congressional correspondence - including constituent mail - please provide me with an information copy. We'll develop an interim response as appropriate depending on the nature and the volume of incoming mail.

Please call if you have any questions. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

USA Patriot Act
Summary of Sunset Provisions

The following provisions are scheduled to sunset on December 31, 2005:

Section 201 & 202 - Expanded Title III predicates

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing). Due to the timing and statutory placement of these two additional predicate offenses, it is likely that these are now included in the sunset provision.

Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. The Homeland Security Act later authorized disclosure to foreign investigative or intelligence officials and to any federal, state, local, and foreign official when it reveals a threat of attack. The termination of the Patriot Act provision would have absurd results. It would eliminate our ability to share foreign intelligence information derived from a Title III with federal intelligence officials, while retaining the ability to share the same information with foreign intelligence officials. [redacted] b2 [redacted] Only if the information constituted a threat of attack, could it be shared with federal intelligence officials.

Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. The Homeland Security Act also added foreign intelligence and investigative officials to the list of receiving officials. Due to the placement of the Homeland Security Act amendments, the Congressional Research Service (CRS) has concluded that these disclosure provisions will also terminate if 203(d) is allowed to sunset.

Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

Prior to the Patriot Act, federal statutes governing the use of criminal investigative wiretaps stated that the interception of wire or oral communications for foreign intelligence purposes should be governed by the provisions of the Foreign Intelligence Surveillance Act (FISA), rather than Title III. This provision, however, did not refer to electronic

communications. As a result, it was arguably unclear whether the interception of electronic communications, such as e-mail messages, for foreign intelligence purposes was governed by FISA or Title II (or both). Section 204 clarified the uncertainty by amending Title 18 to confirm that in foreign intelligence investigations, it is FISA, and not Title III, that governs the interception of electronic communications as well as wire and oral communications.

Section 206 - Roving FISA Surveillance (S)

When a FISA target's actions have the effect of thwarting surveillance, such as b[redacted] the Court can issue an order (S)
directing as y[redacted] etc., to effect the
authorized electronic surveillance. This allows the FBI to go directly to the new carrier and b1
establish surveillance on the authorized target without having to return to the Court for a new
secondary order.

Section 207 - Extended Duration for Certain FISAs

Section 207 extends the standard duration for several categories of FISA orders.

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 b2
U.S.C. § 2703[redacted] Previously, some courts had required a Title III order to obtain b7E
stored voice mail. The language in Section 209 of the Patriot Act eliminated the distinction in
the definitions for "wire communication" and "electronic communication" that was relied on in a
2004 First Circuit opinion (United States v. Councilman) to minimize privacy protection for e-
mail. As such, should Congress allow this provision to sunset[redacted] b5

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury. The Homeland Security Act modified this provision as it relates to the content of communications, but not as it relates to the records held by a service provider. For this reason, the Congressional Research Service has concluded that only those provisions relating to the voluntary disclosure of records is subject to the sunset provision

Section 214 - FISA Pen/Trap Authority

FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications (i.e. Internet), comparable to the criminal pen/trap provision.

Section 215 - Access to Business Records under FISA

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records [redacted] b2 [redacted] to include "any tangible things (including books, records, papers, b7E documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

Section 217 - Interception of Computer Trespasser Communications

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

Section 218 - Change in the "Primary Purpose" Standard of FISA

Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal

investigators or prosecutors without putting their FISAs at risk.

Section 220 - Nationwide Search Warrants for Electronic Evidence

Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

Section 223 - Civil Liability for Certain Unauthorized Disclosures

Prior to the passage of the Patriot Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Section 225 - Immunity for Compliance with FISA Wiretap

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISC to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent or a foreign power, such as international terrorists and spies. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of [redacted] to carry out such court orders. Prior to the passage of the Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected [redacted] assisting the government in carrying out wiretap and surveillance orders issued by the FISC under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such [redacted] will comply with orders issued by the FISC without delay.

b2
b7E

From: [redacted] (OGC) (FBI)
Sent: Thursday, March 03, 2005 12:04 PM
To: [redacted] (OCA) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: Sunset Provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] - If it is still helpful, attached please find two bullets for the Director. I focused the thoughts on information sharing and investigating internet based information for all types of crimes. The bullets emphasize the resulting impact if these provisions expire. b6 b7C

[redacted] also noted that it might be worth having the Director seek helpful examples using delayed notice search warrants, as that provision, while not a sunset provision, has come under much attack.

Finally, I did not address the FISA primary purpose standard (Section 218), but note that section's importance to the whole information sharing issue. Has anyone in OIPR (or otherwise) opined on what would happen to the FISA standard if that section were to expire? Would the FISA court's opinion be altered? Since I do not work FISA issues, I have refrained from commenting on that provision. However, I wonder if that isn't the single most important sunset provision. It might get a lot of attention if someone were to note how the landscape would change if that provision is allowed to expire.

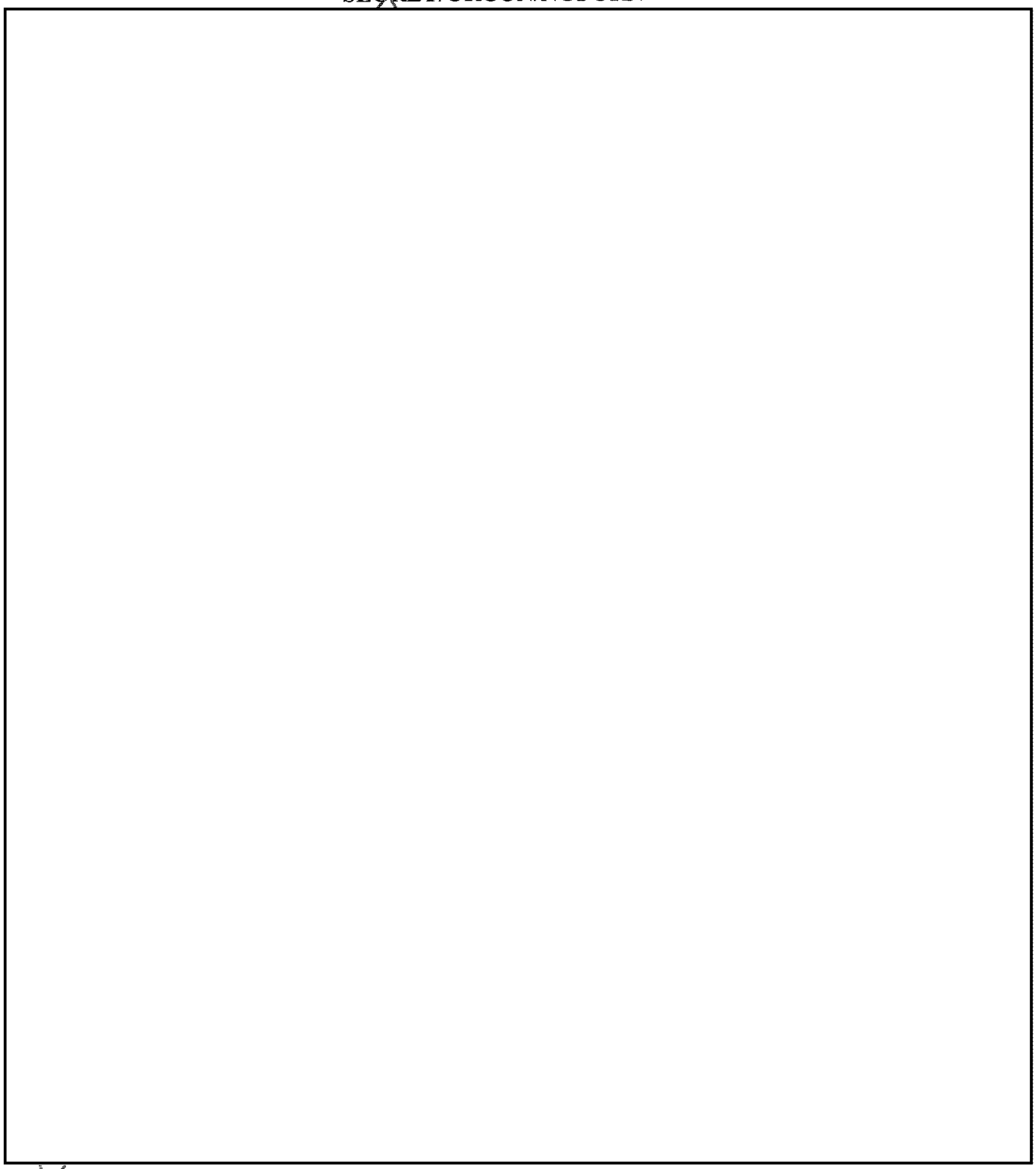
If you have any other questions, or need additional assistance on the sunset "battle," please feel free to contact me.

Thanks --

[redacted] b2
Assistant General Counsel b6
Investigative Law Unit
Office of the General Counsel b7C
[redacted]

UNCLASSIFIED

b5



(S/NF,OC)

b1
b7A
b6
b7C
b5

(U)

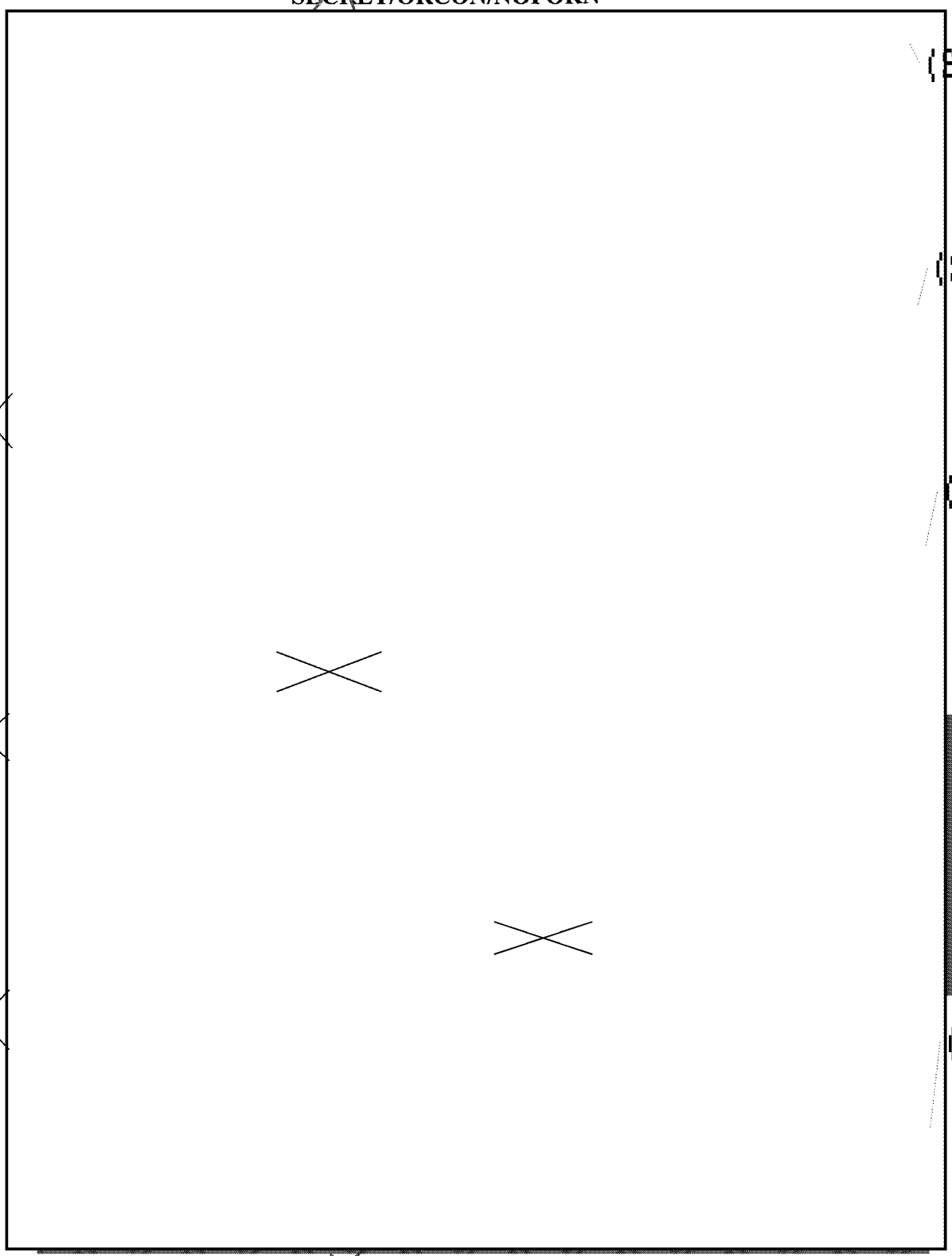
(U)

(S)

(S)

(S)

(S)

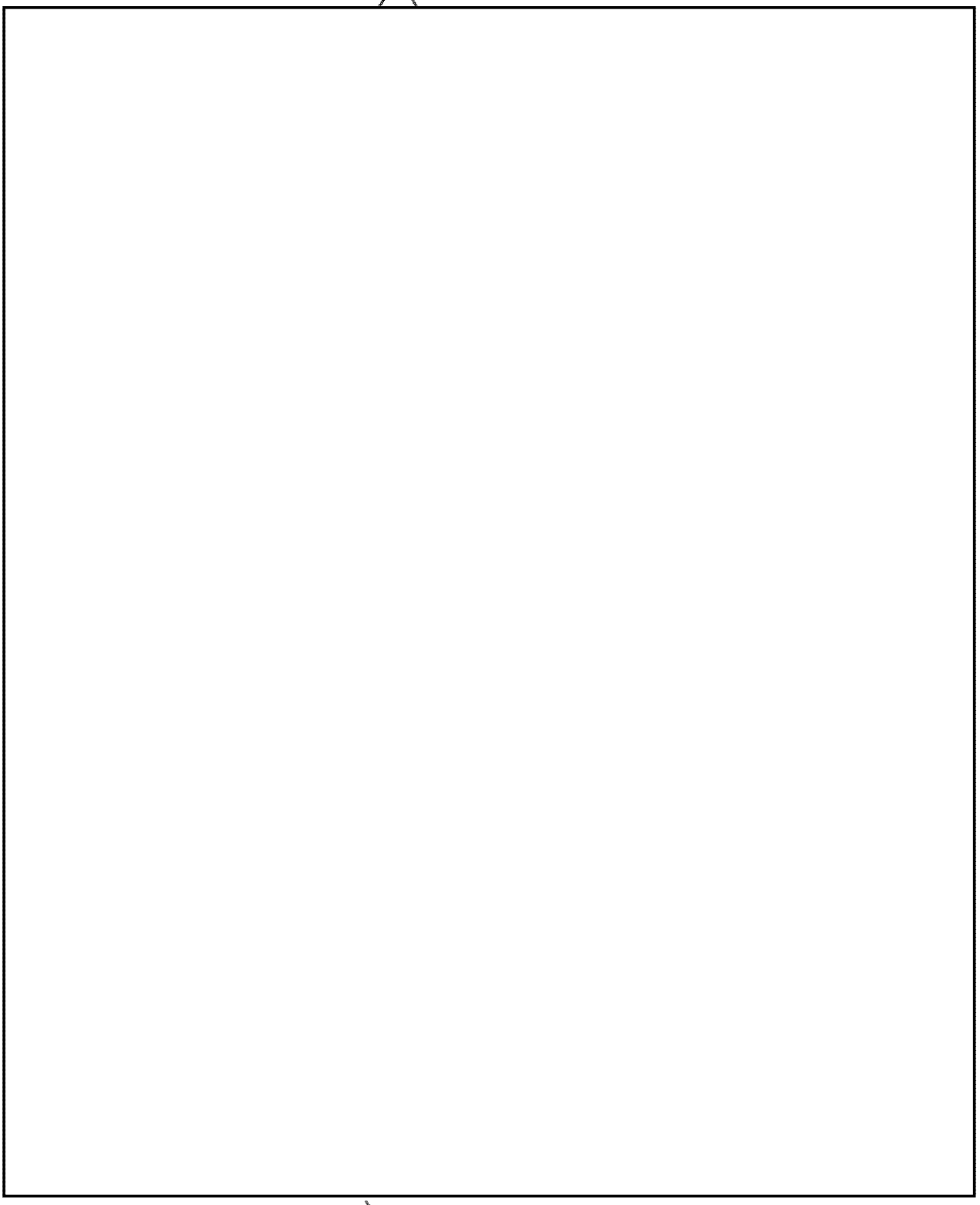


b1
b2
b5
b6
b7C
b7D
b7E
b7A

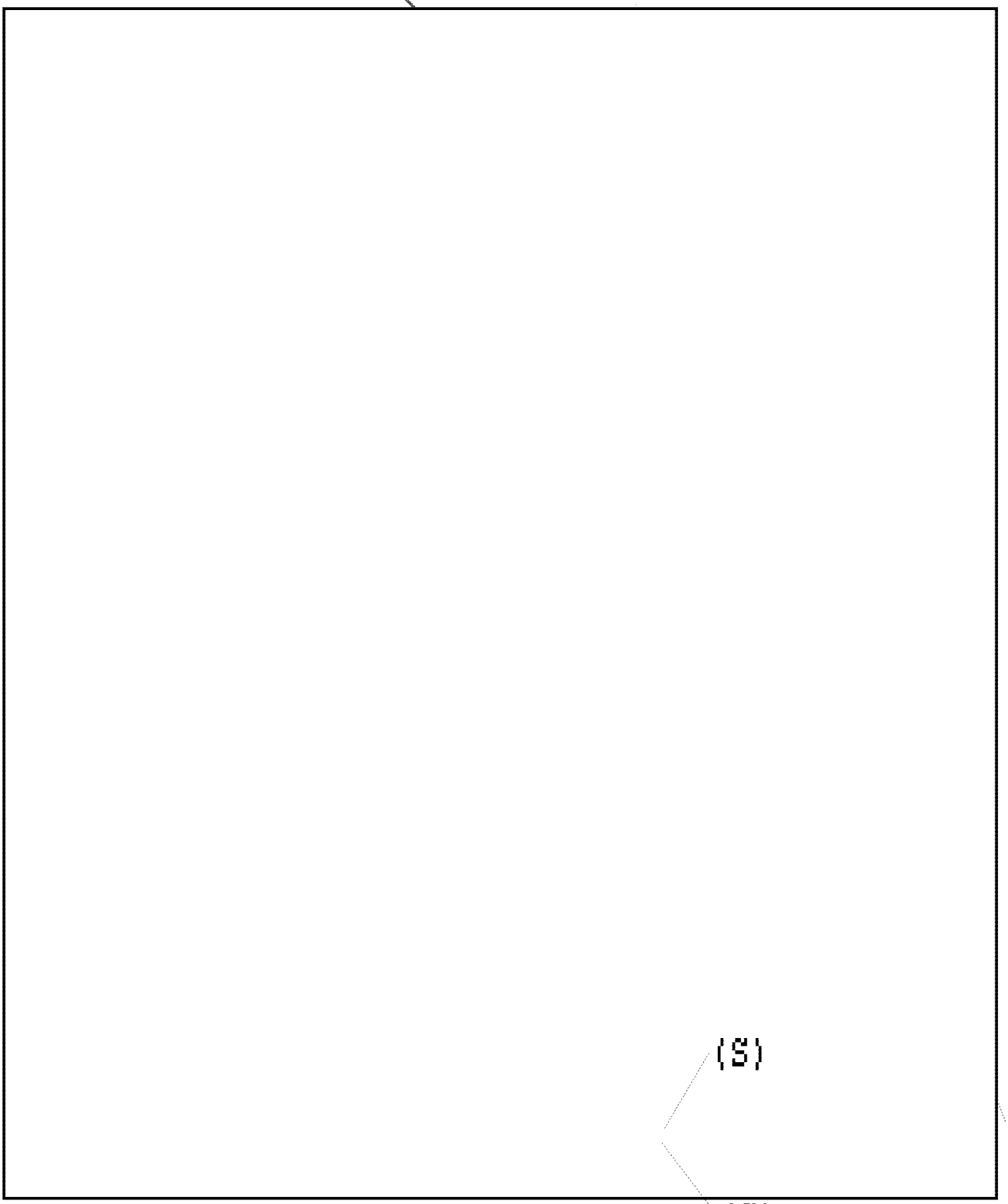
(S)

b1
b2
b6
b7C
b7E
b7A
b5

(S)



b2
b7A
b6
b7C
b5
b7E

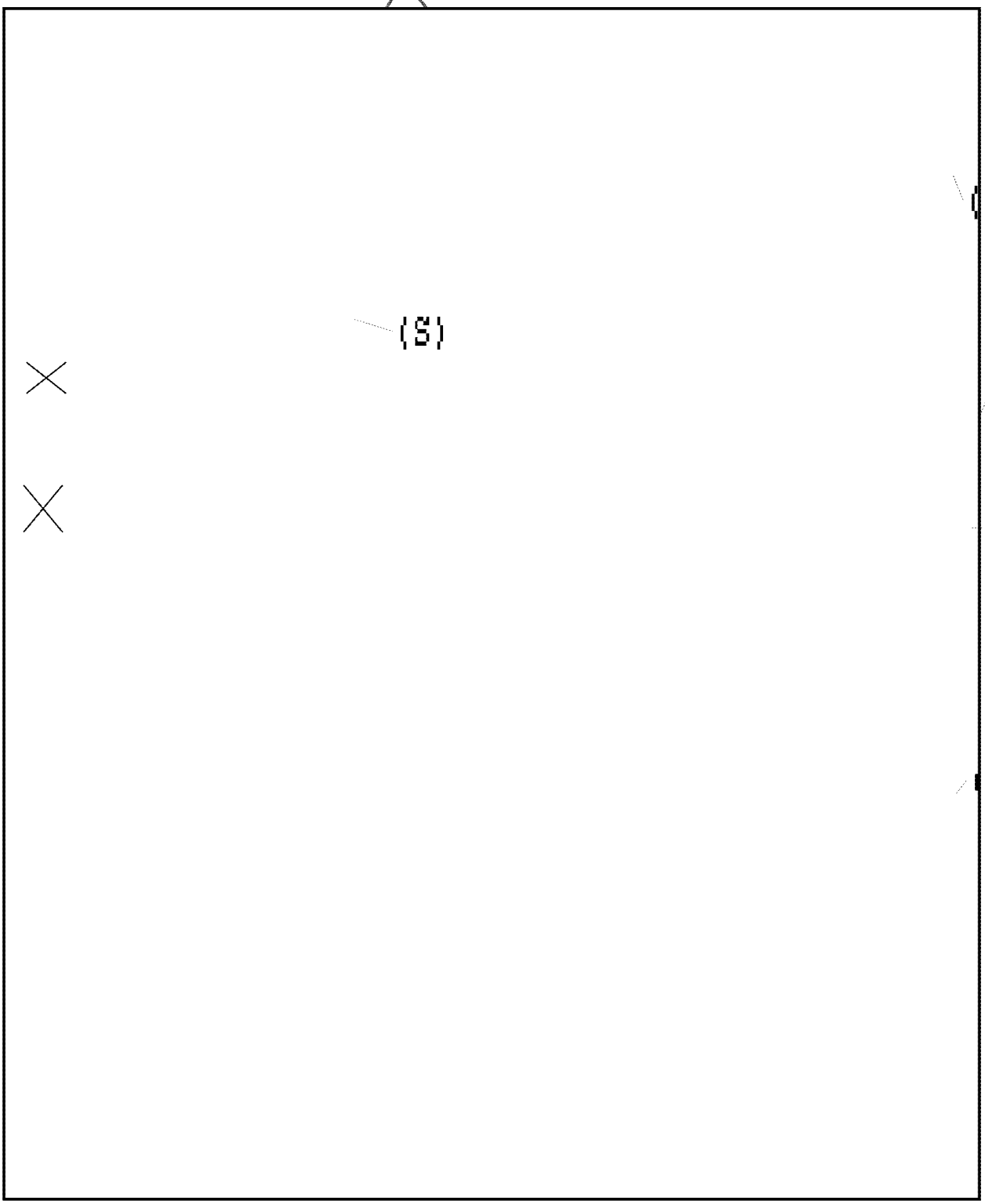


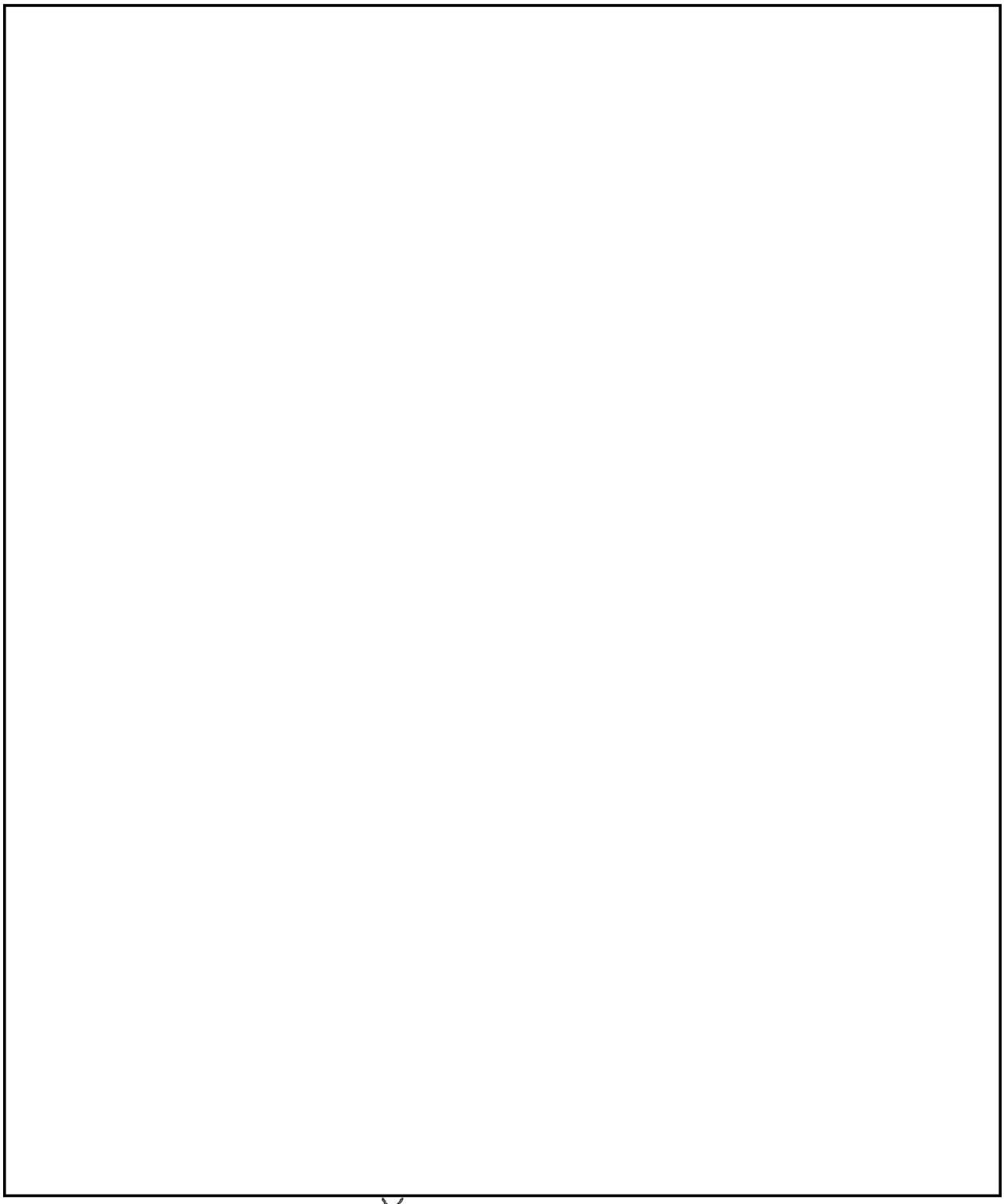
b1
b2
b6
b7A
b7C
b7E
b5

(S)

(S)

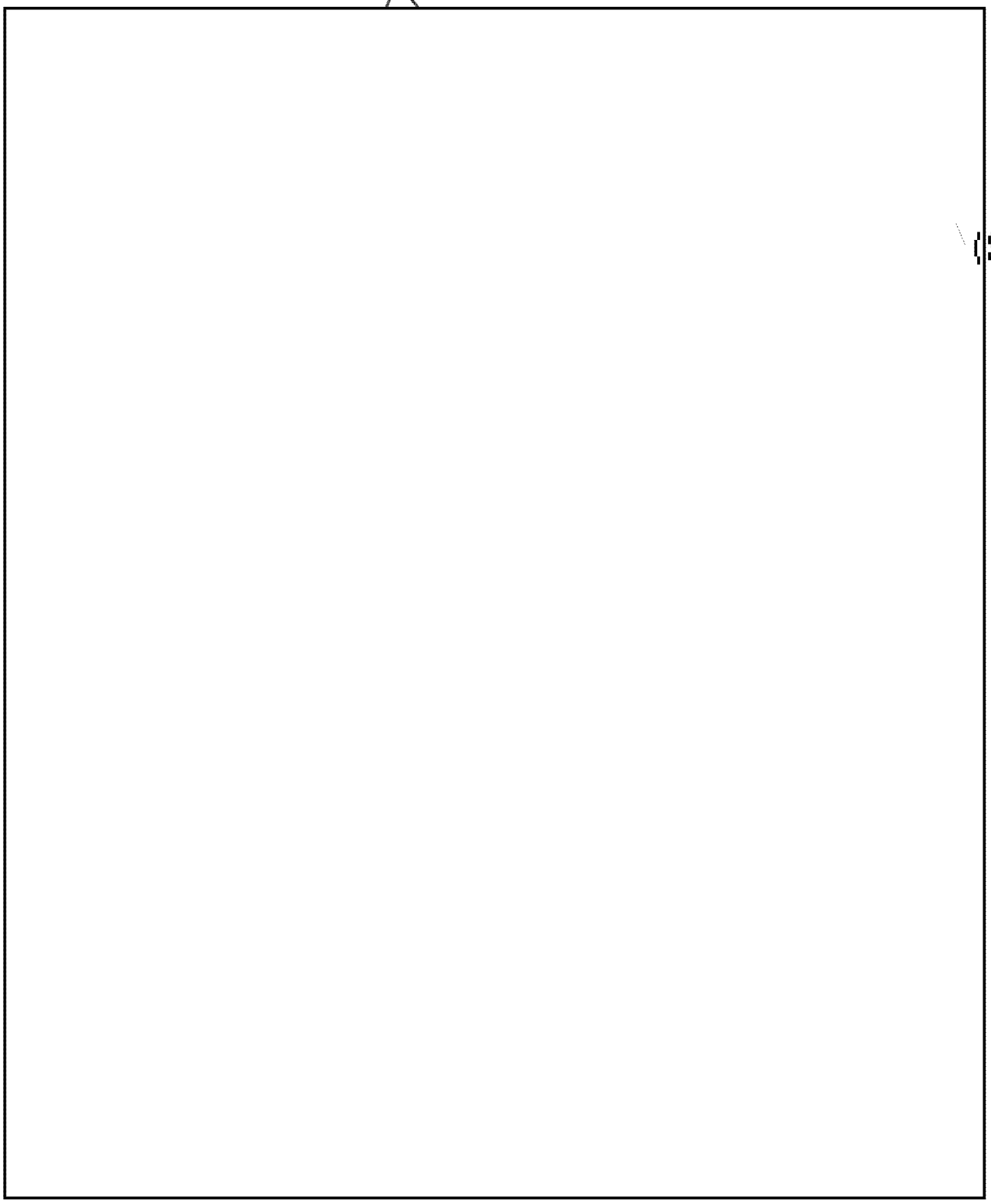
(S)


(S)
(S)
(S)
(S)
(S)
b1
b2
b5
b6
b7C
b7E



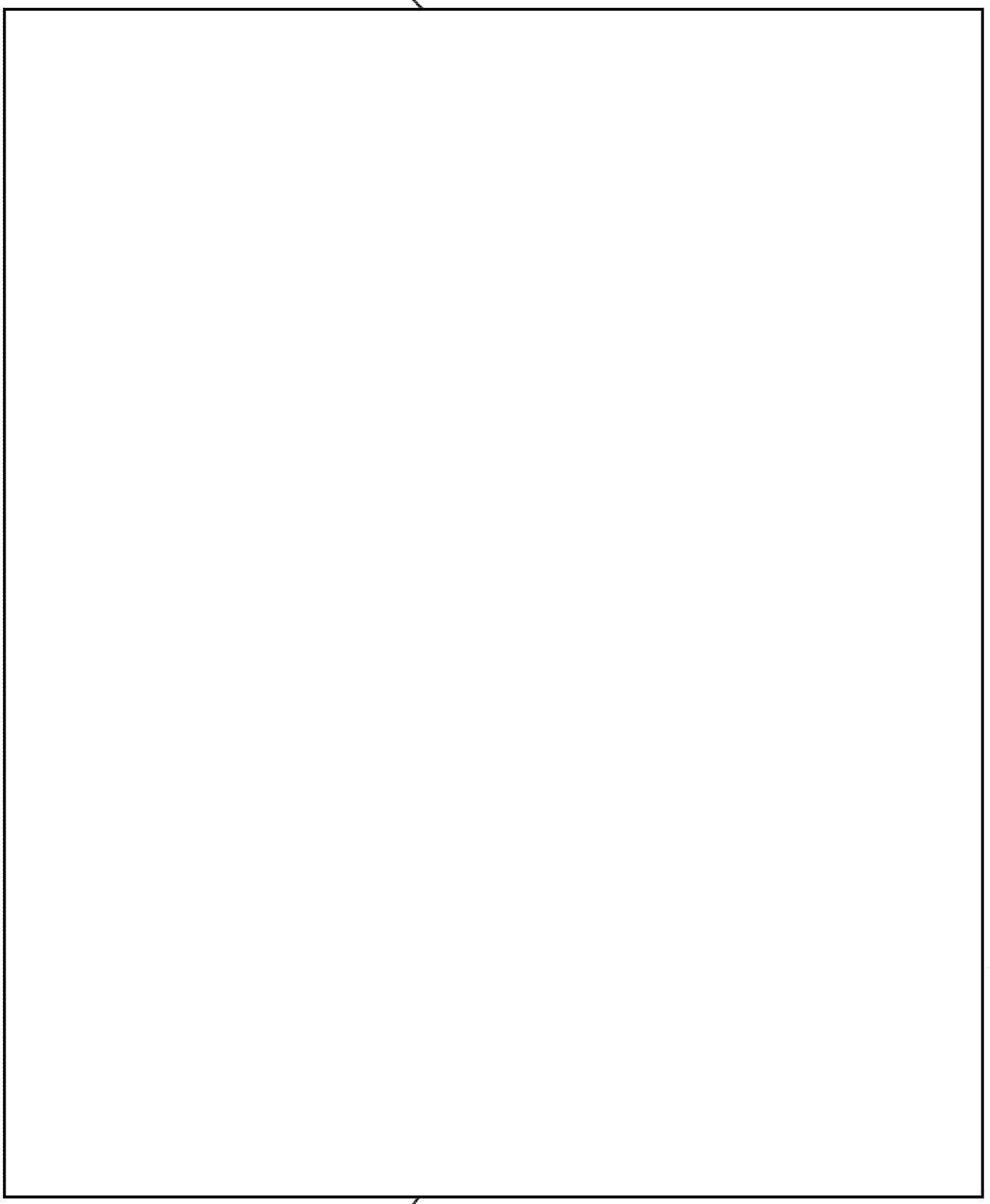
b7A

b5

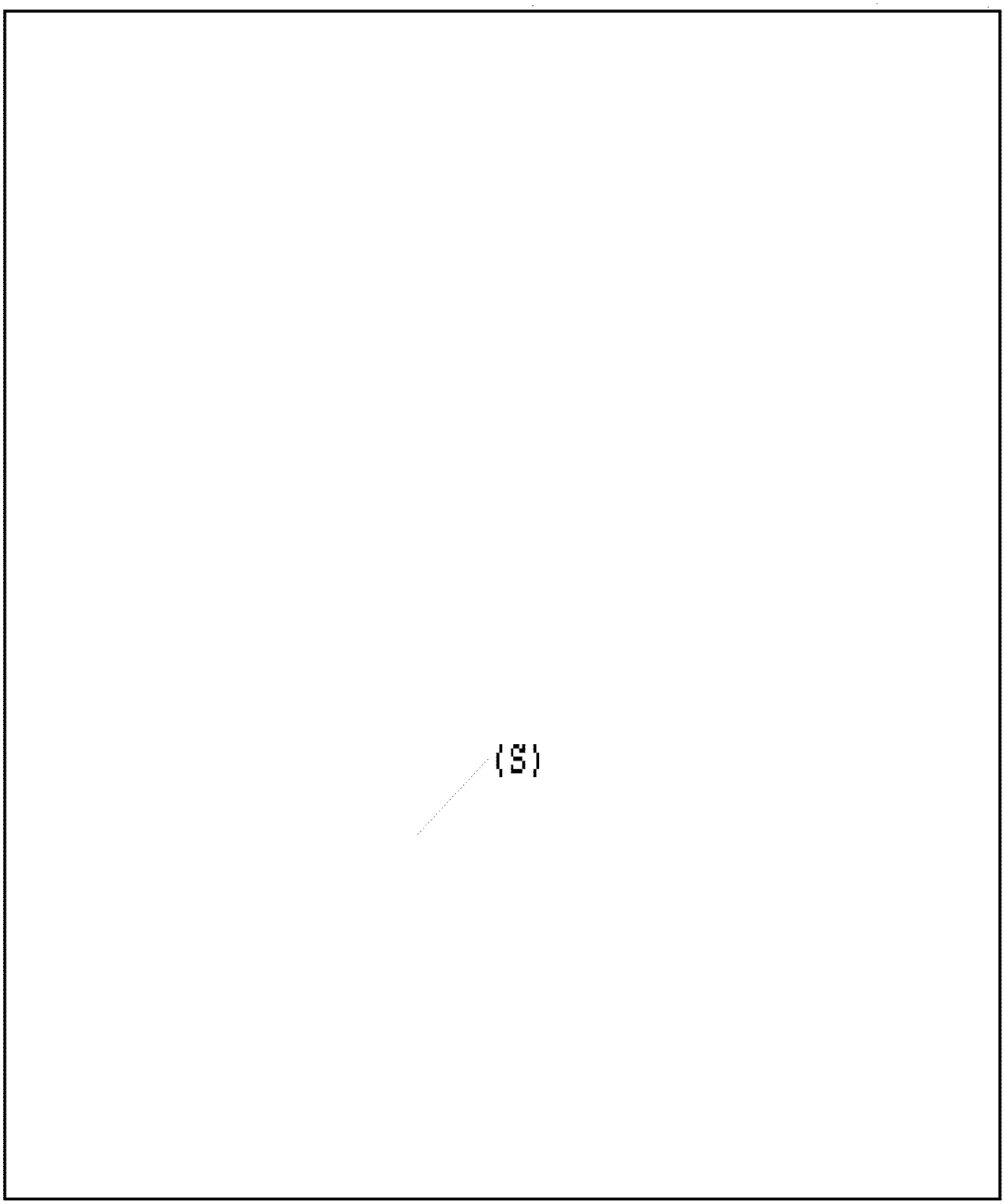


(S)

b1
b2
b7E
b5

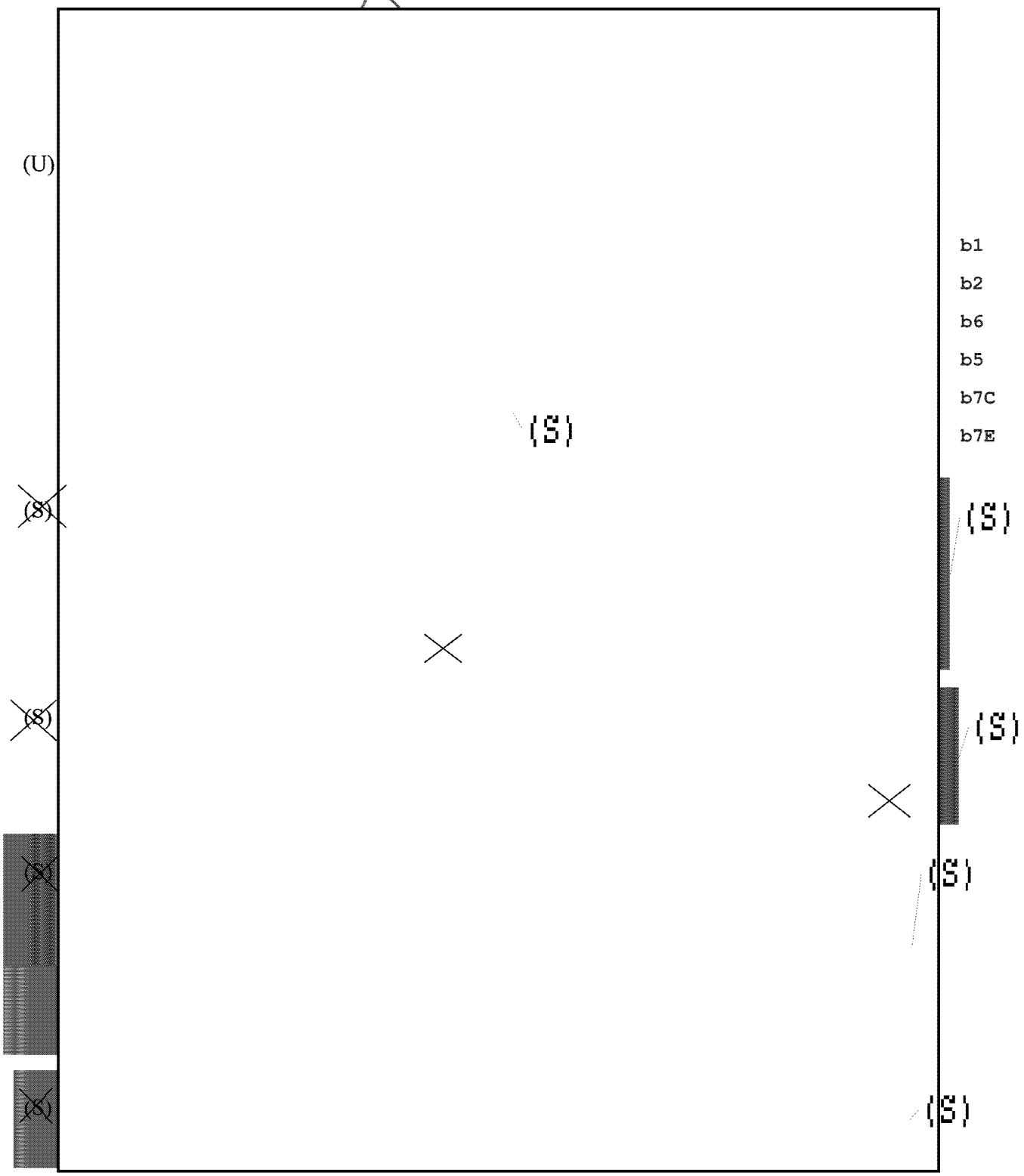


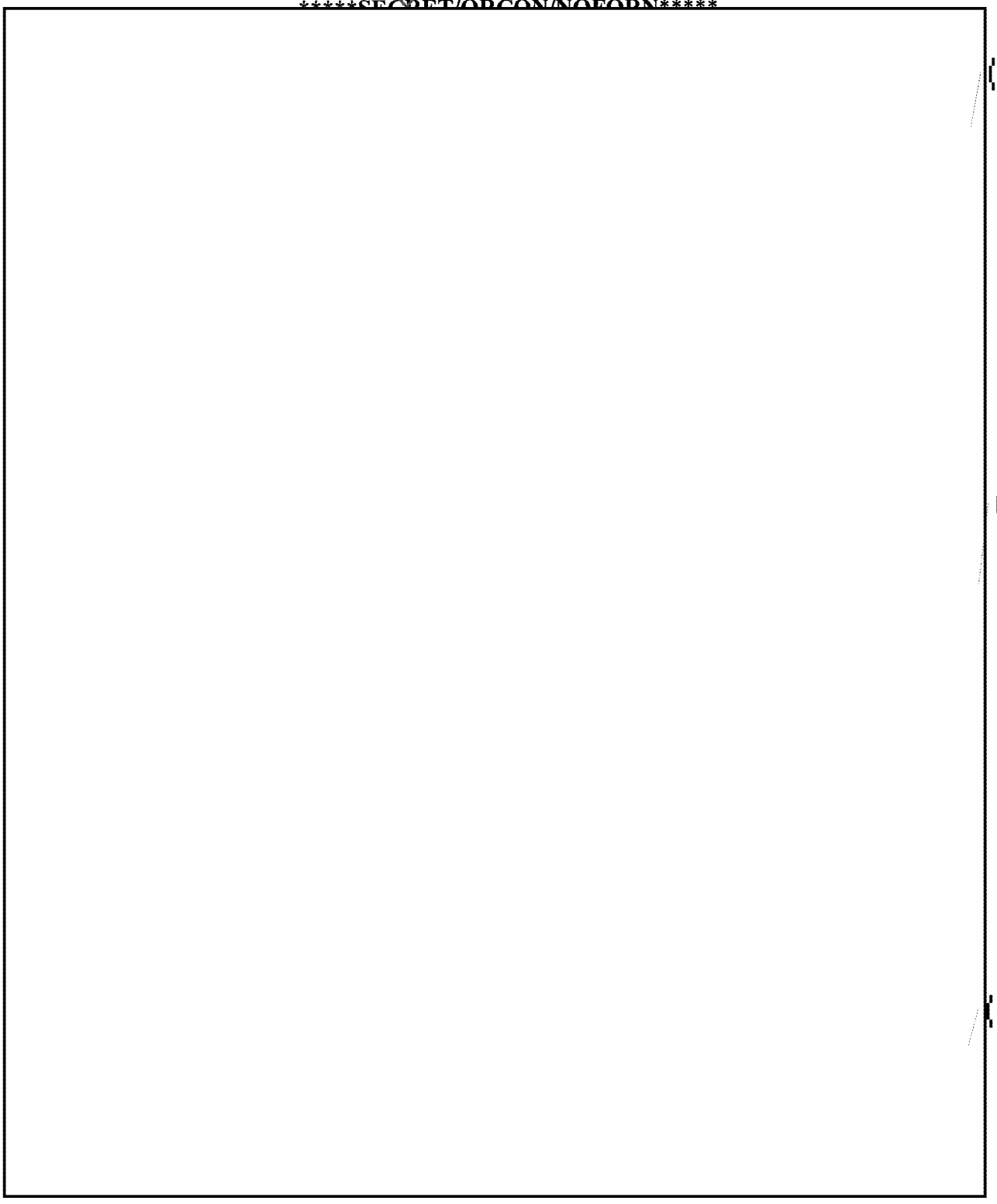
b2
b5
b6
b7C
b7D
b7E
b7A



(S)

b1
b2
b7E
b6
b7C
b7A
b5


(U)
b1
b2
b6
b5
b7C
b7E
(S)
(S)
(S)
(S)
(S)
(S)
(S)



(S)

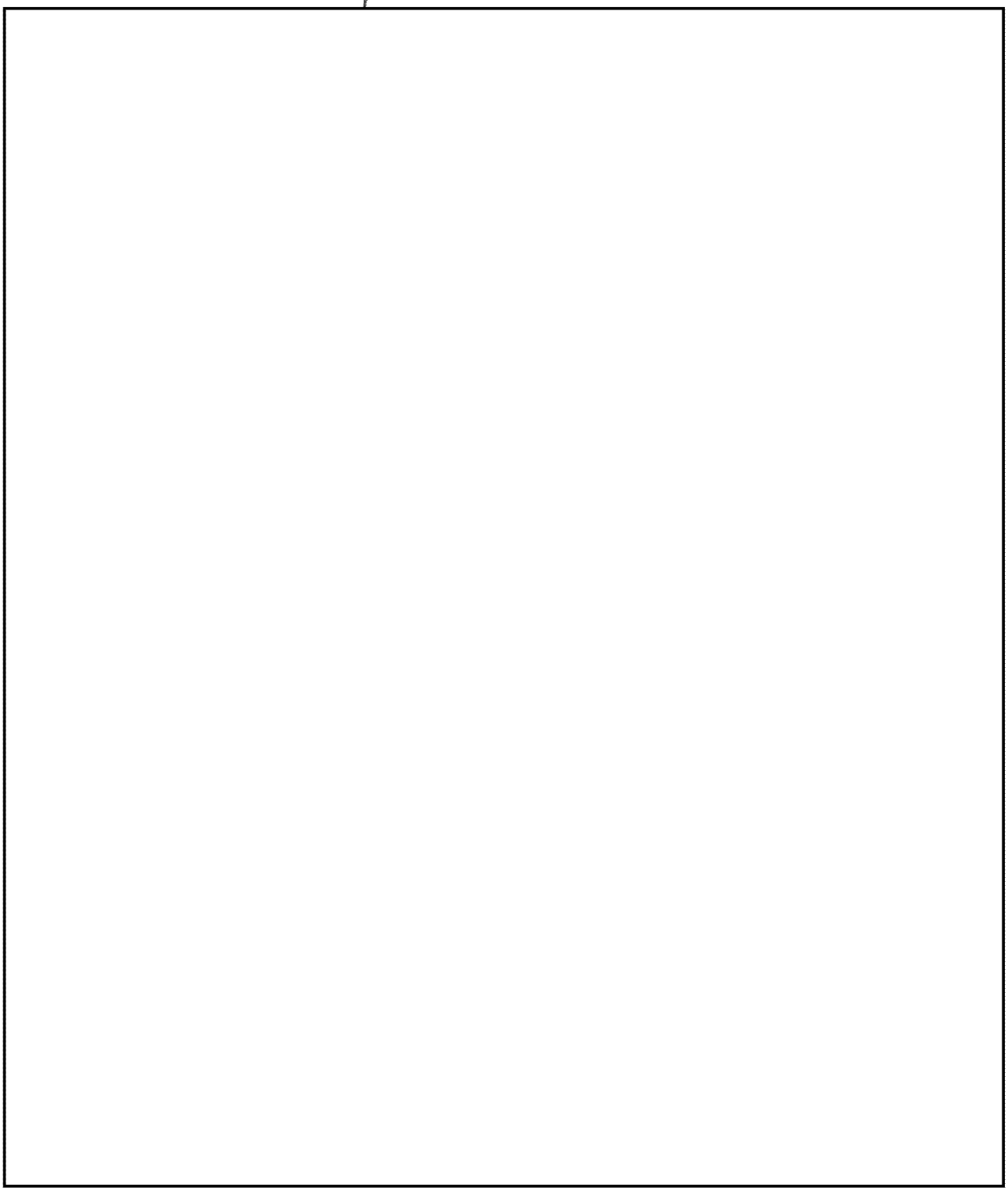
(S)

b1
b2
b5
b6
b7C
b7E

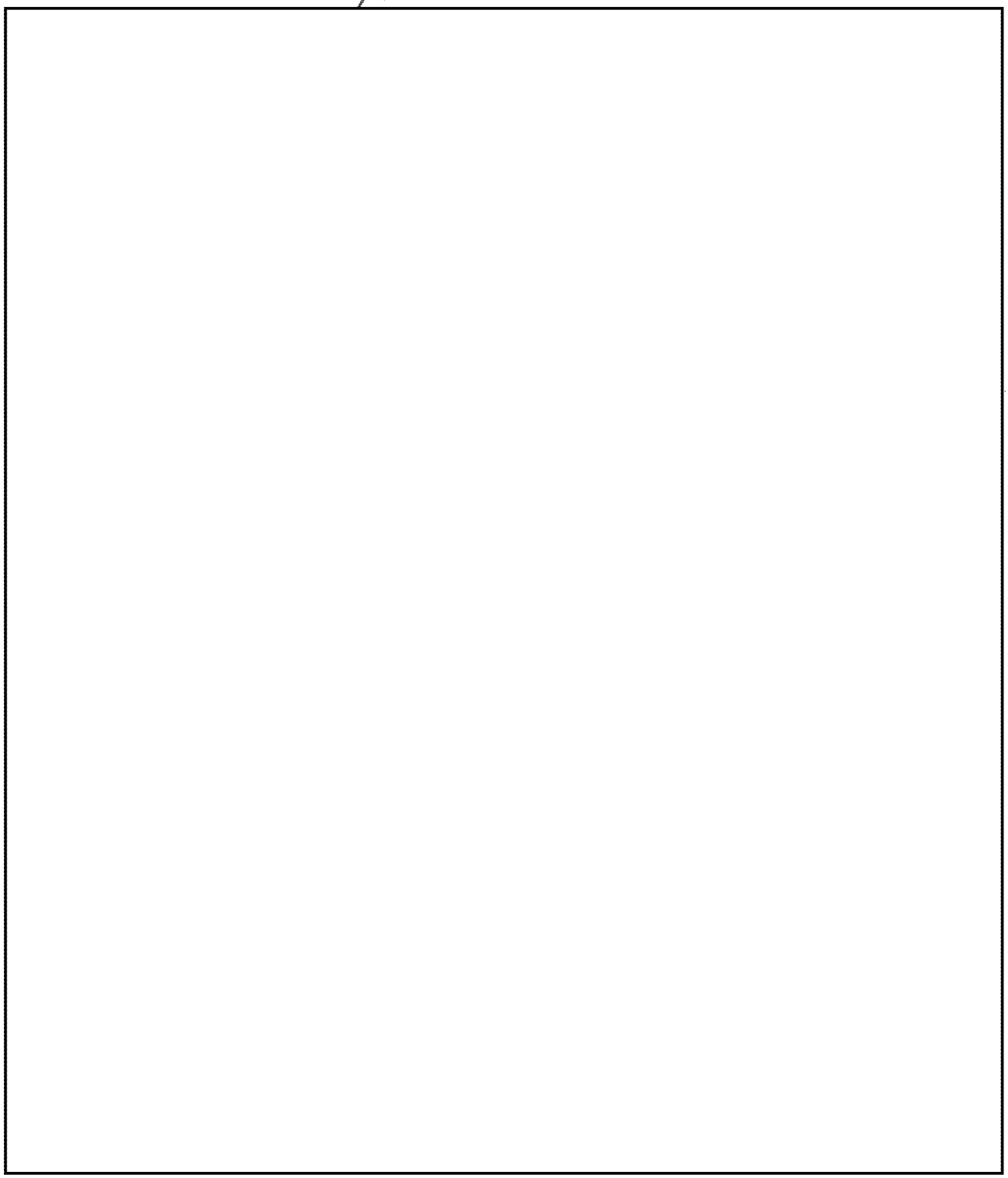
(S)

(S)

b1
b2
b7E
b5
b7A



b2
b7E
b5
b7D



b2
b7E
b7A
b6
b7C
b7D
b5

b2
b7E
b7A
b6
b7C
b7D
b5

b5
b6
b7A
b7C

(U)

(U)

(U)

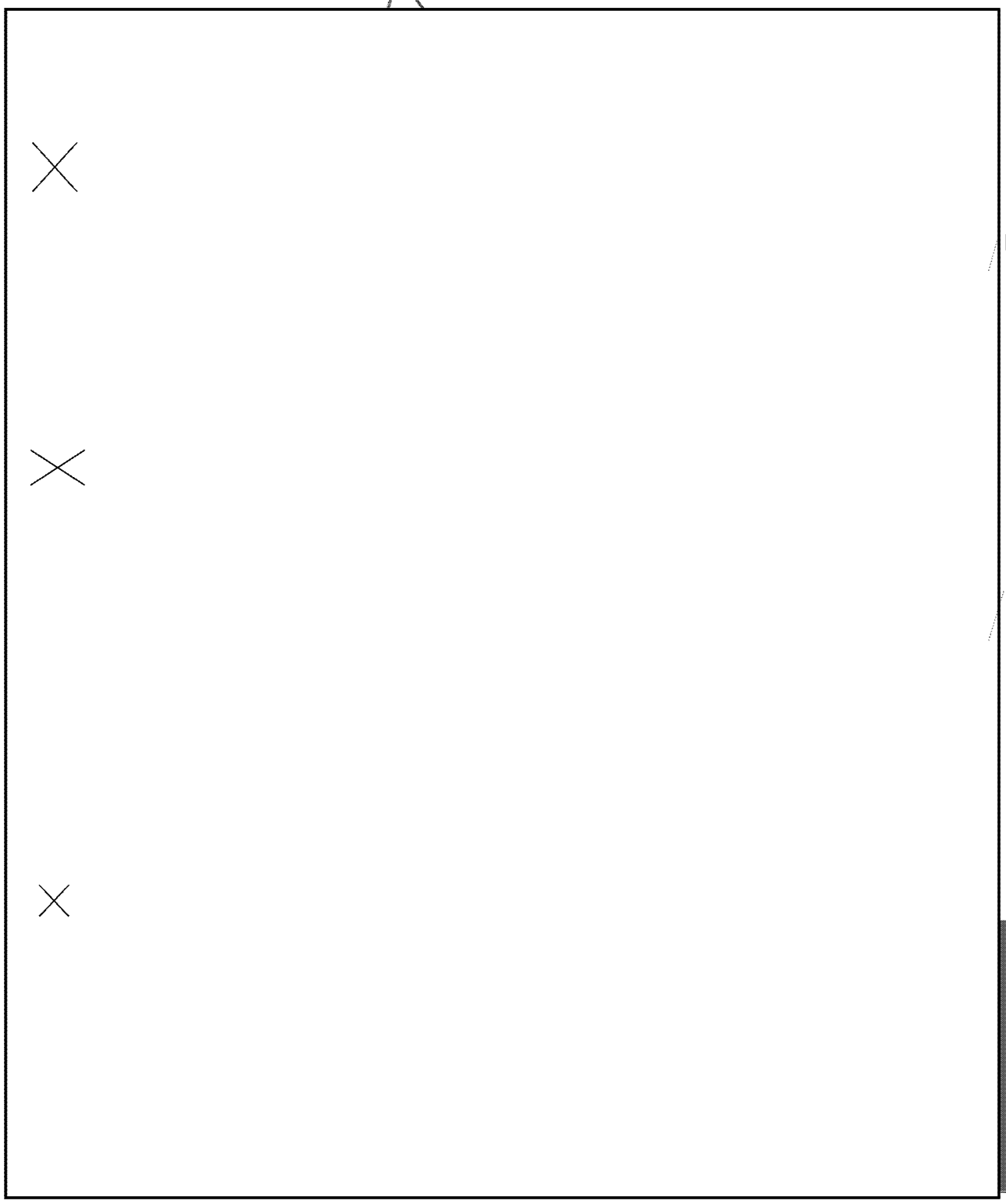
(U)

(S)

b7A

b5

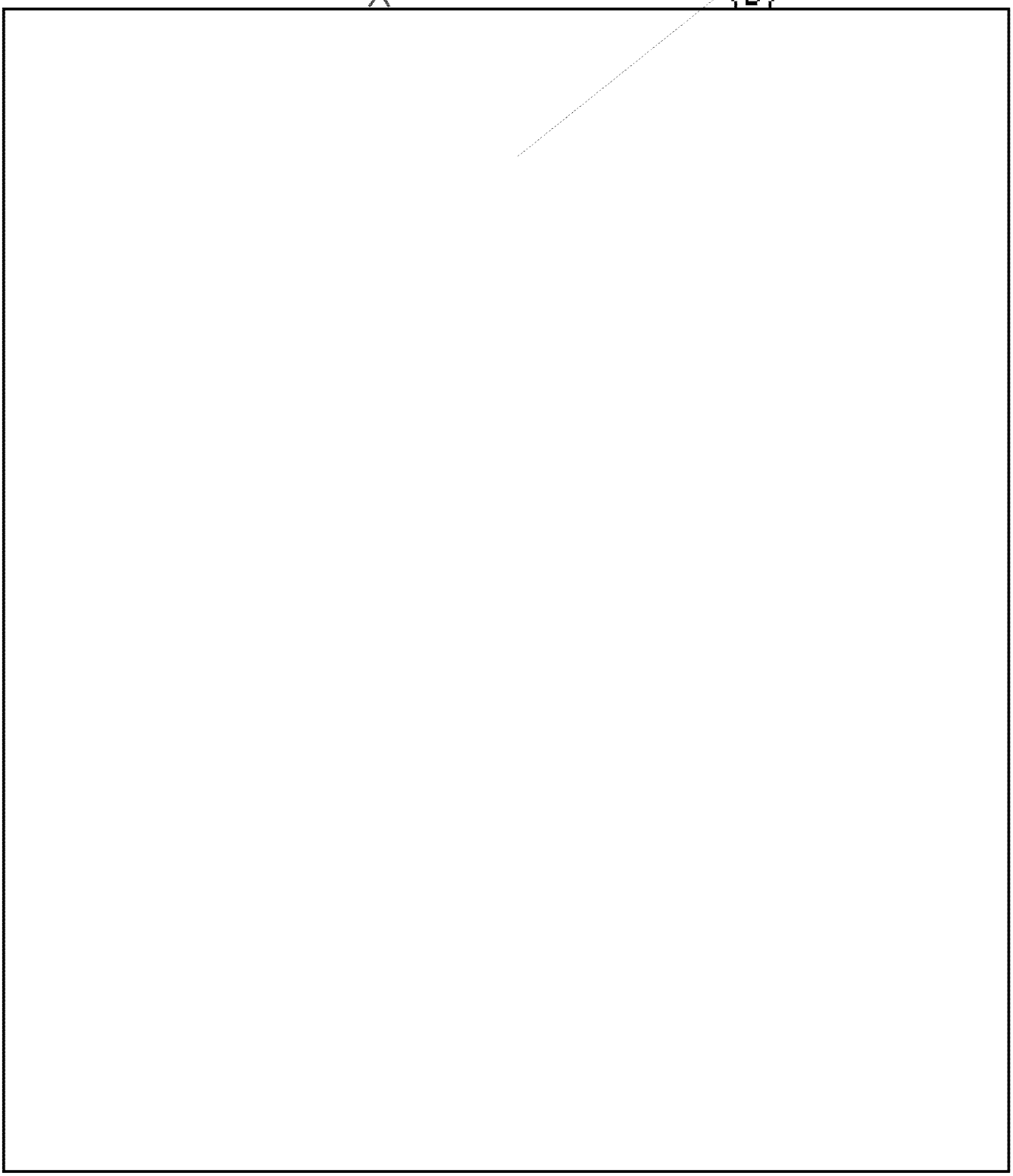
b1
b2
b7E
b5



(S)

(S)

(S)



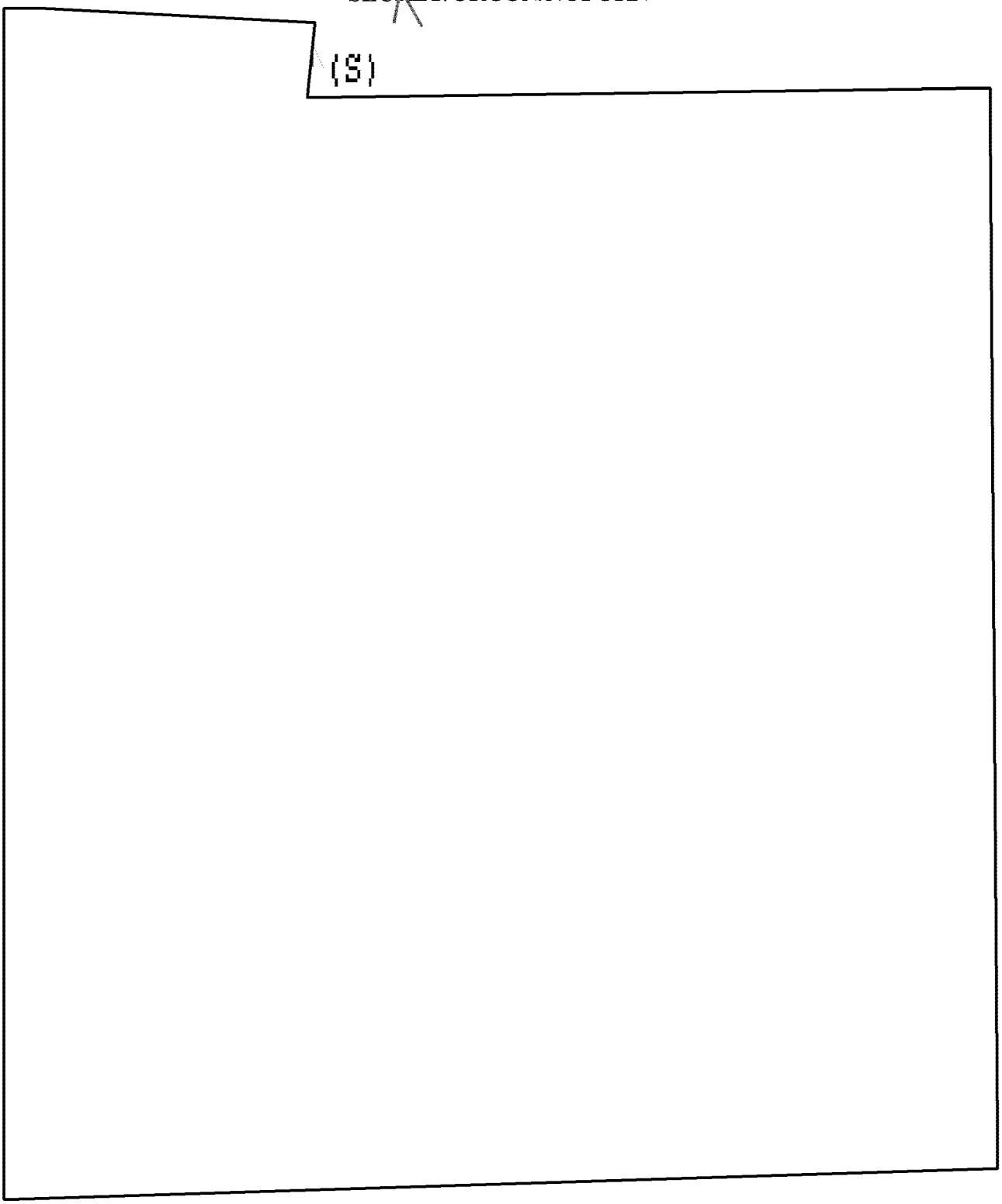
b1
b2
b7E
b5
b6
b7C
b7A

(S)

b1
b2
b5

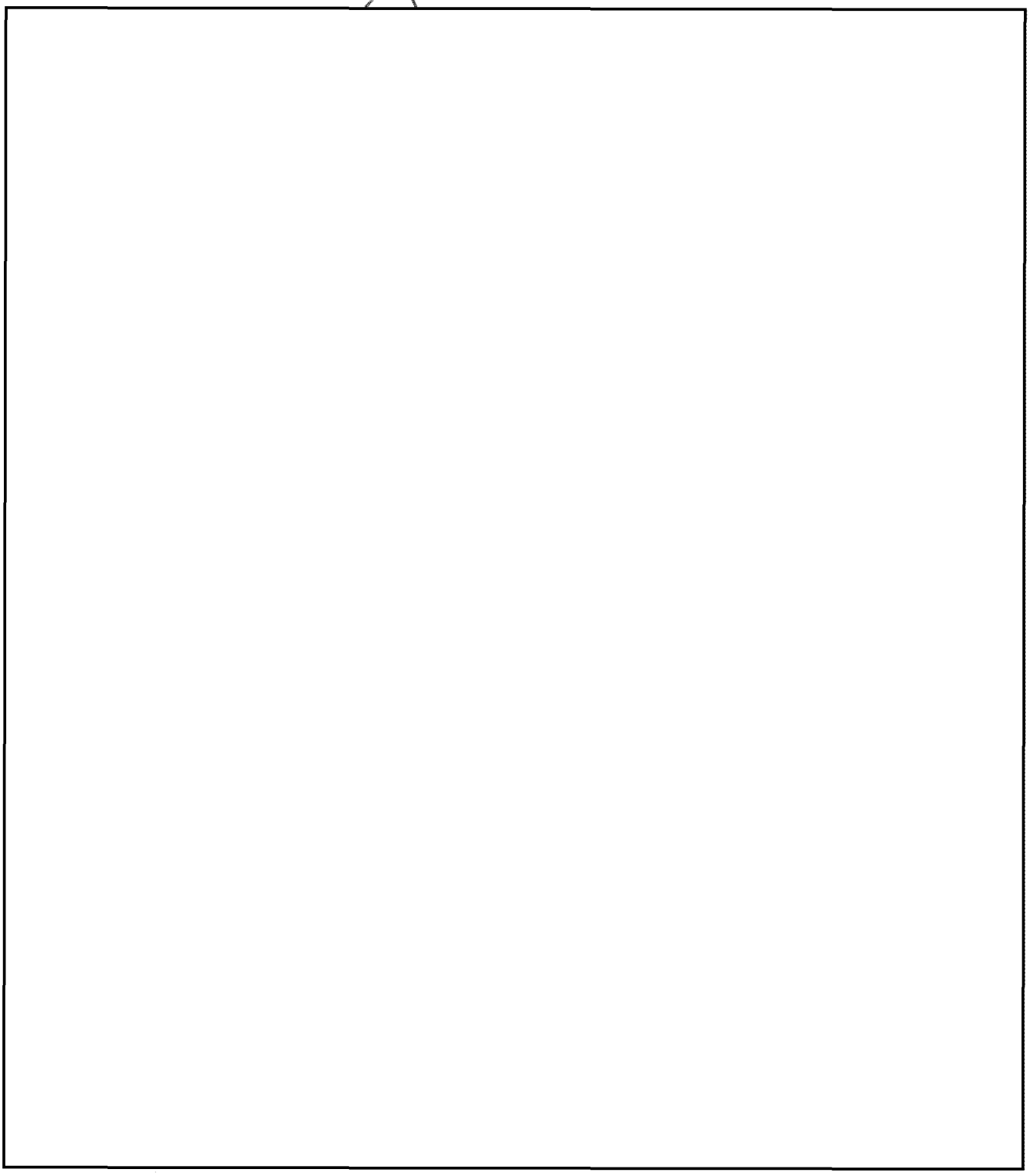
(S)

(S)

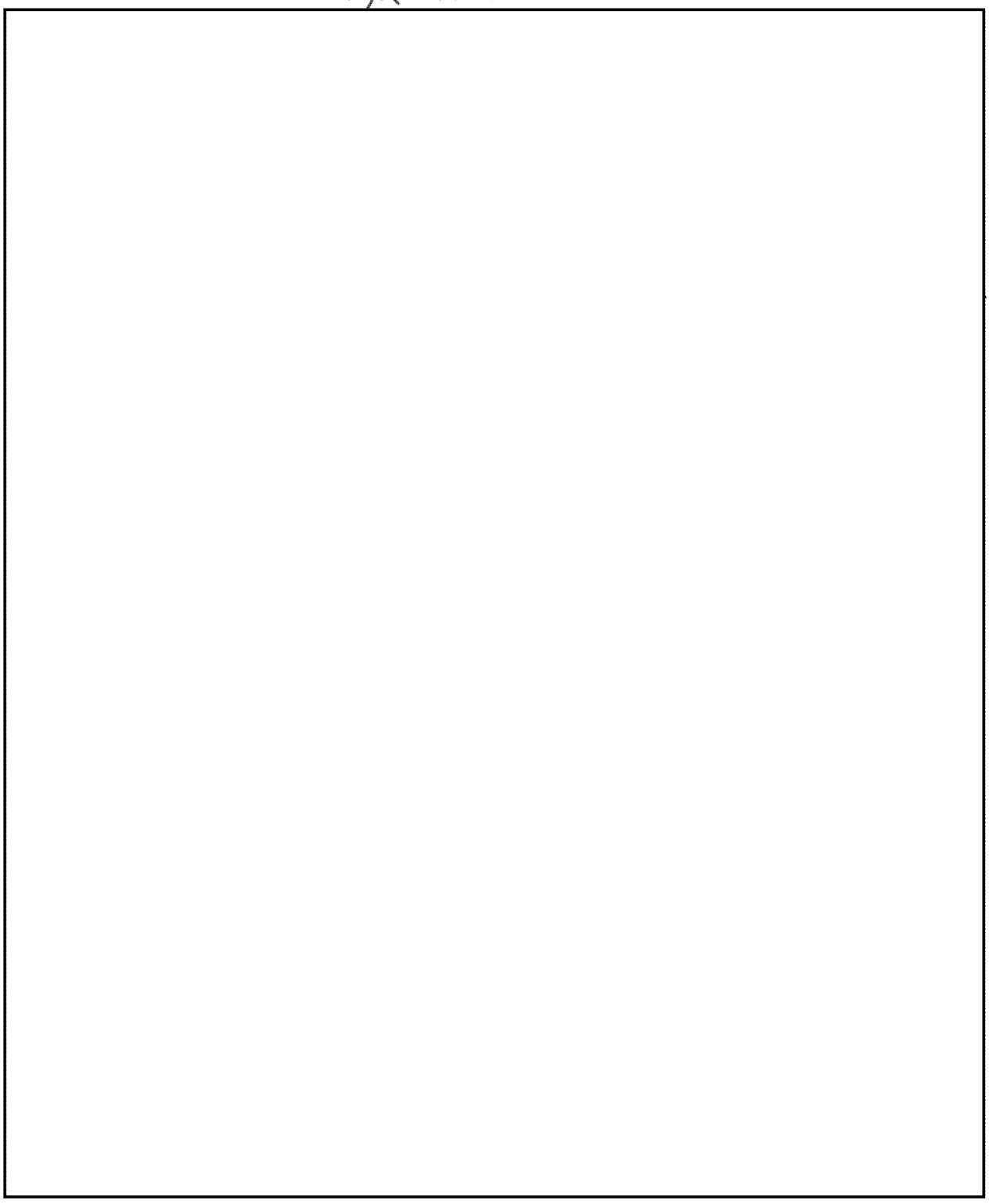


b1
b2
b7E
b5
b7A

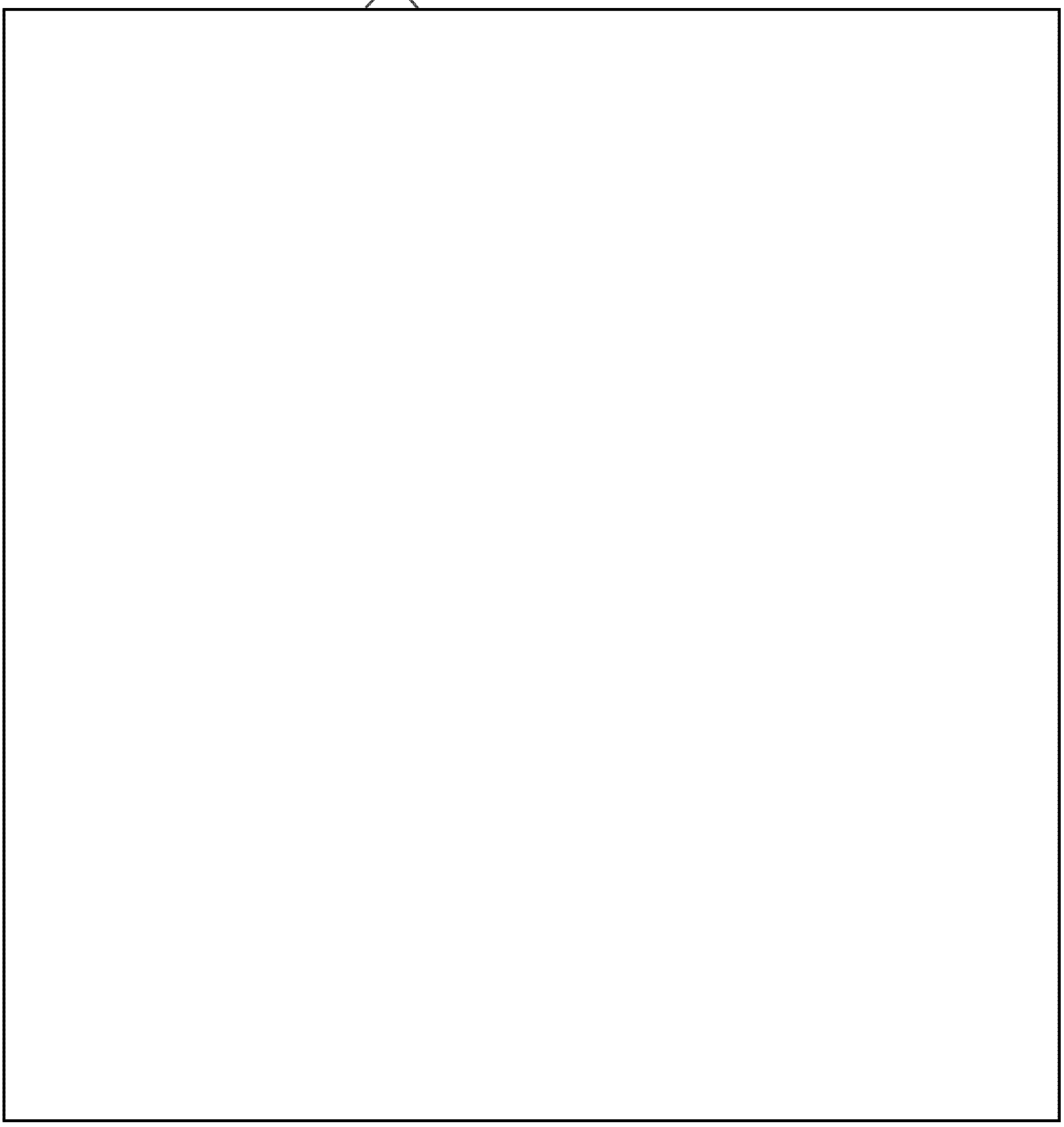
b2
b7E
b5
b6
b7C
b7A



b5
b2
b7E
b6
b7C
b7D
b7A



b2
b7E
b6
b7C
b7A
b5



b6
b7C
b7A
b5

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 450
Page 3 ~ Referral/Direct DOJ
Page 4 ~ Referral/Direct DOJ
Page 5 ~ Referral/Direct DOJ
Page 6 ~ Referral/Direct DOJ
Page 7 ~ Referral/Direct DOJ
Page 8 ~ Referral/Direct DOJ
Page 9 ~ Referral/Direct DOJ
Page 10 ~ Referral/Direct DOJ
Page 11 ~ Referral/Direct DOJ
Page 12 ~ Referral/Direct DOJ
Page 13 ~ Referral/Direct DOJ
Page 14 ~ Referral/Direct DOJ
Page 15 ~ Referral/Direct DOJ
Page 16 ~ Referral/Direct DOJ
Page 17 ~ Referral/Direct DOJ
Page 22 ~ Referral/Direct DOJ
Page 23 ~ Referral/Direct DOJ
Page 25 ~ Referral/Direct DOJ
Page 26 ~ Referral/Direct DOJ
Page 27 ~ Referral/Direct DOJ
Page 28 ~ Referral/Direct DOJ
Page 29 ~ Referral/Direct DOJ
Page 30 ~ Referral/Direct DOJ
Page 31 ~ Referral/Direct DOJ
Page 32 ~ Referral/Direct DOJ
Page 33 ~ Referral/Direct DOJ
Page 34 ~ Referral/Direct DOJ
Page 35 ~ Referral/Direct DOJ
Page 36 ~ Referral/Direct DOJ
Page 37 ~ Referral/Direct DOJ
Page 38 ~ Referral/Direct DOJ
Page 39 ~ Referral/Direct DOJ
Page 40 ~ Referral/Direct DOJ
Page 41 ~ Referral/Direct DOJ
Page 42 ~ Referral/Direct DOJ
Page 43 ~ Referral/Direct DOJ
Page 44 ~ Referral/Direct DOJ
Page 45 ~ Referral/Direct DOJ
Page 46 ~ Referral/Direct DOJ
Page 47 ~ Referral/Direct DOJ
Page 48 ~ Referral/Direct DOJ
Page 49 ~ Referral/Direct DOJ
Page 50 ~ Referral/Direct DOJ
Page 51 ~ Referral/Direct DOJ

Page 52 ~ Referral/Direct DOJ
Page 53 ~ Referral/Direct DOJ
Page 54 ~ Referral/Direct DOJ
Page 55 ~ Referral/Direct DOJ
Page 56 ~ Referral/Direct DOJ
Page 57 ~ Referral/Direct DOJ
Page 58 ~ Referral/Direct DOJ
Page 59 ~ Referral/Direct DOJ
Page 60 ~ Referral/Direct DOJ
Page 61 ~ Referral/Direct DOJ
Page 62 ~ Referral/Direct DOJ
Page 63 ~ Referral/Direct DOJ
Page 64 ~ Referral/Direct DOJ
Page 65 ~ Referral/Direct DOJ
Page 66 ~ Referral/Direct DOJ
Page 67 ~ Referral/Direct DOJ
Page 68 ~ Referral/Direct DOJ
Page 69 ~ Referral/Direct DOJ
Page 70 ~ Referral/Direct DOJ
Page 71 ~ Referral/Direct DOJ
Page 72 ~ Referral/Direct DOJ
Page 73 ~ Referral/Direct DOJ
Page 74 ~ Referral/Direct DOJ
Page 75 ~ Referral/Direct DOJ
Page 76 ~ Referral/Direct DOJ
Page 77 ~ Referral/Direct DOJ
Page 78 ~ Referral/Direct DOJ
Page 79 ~ Referral/Direct DOJ
Page 80 ~ Referral/Direct DOJ
Page 81 ~ Referral/Direct DOJ
Page 82 ~ Referral/Direct DOJ
Page 83 ~ Referral/Direct DOJ
Page 84 ~ Referral/Direct DOJ
Page 85 ~ Referral/Direct DOJ
Page 86 ~ Referral/Direct DOJ
Page 87 ~ Referral/Direct DOJ
Page 88 ~ Referral/Direct DOJ
Page 89 ~ Referral/Direct DOJ
Page 90 ~ Referral/Direct DOJ
Page 91 ~ Referral/Direct DOJ
Page 92 ~ Referral/Direct DOJ
Page 93 ~ Referral/Direct DOJ
Page 94 ~ Referral/Direct DOJ
Page 95 ~ Referral/Direct DOJ
Page 96 ~ Referral/Direct DOJ
Page 97 ~ Referral/Direct DOJ
Page 98 ~ Referral/Direct DOJ
Page 99 ~ Referral/Direct DOJ
Page 100 ~ Referral/Direct DOJ
Page 101 ~ Referral/Direct DOJ
Page 102 ~ Referral/Direct DOJ

Page 103 ~ Referral/Direct DOJ
Page 104 ~ Referral/Direct DOJ
Page 105 ~ Referral/Direct DOJ
Page 106 ~ Referral/Direct DOJ
Page 107 ~ Referral/Direct DOJ
Page 108 ~ Referral/Direct DOJ
Page 109 ~ Referral/Direct DOJ
Page 110 ~ Referral/Direct DOJ
Page 111 ~ Referral/Direct DOJ
Page 112 ~ Referral/Direct DOJ
Page 113 ~ Referral/Direct DOJ
Page 114 ~ Referral/Direct DOJ
Page 115 ~ Referral/Direct DOJ
Page 116 ~ Referral/Direct DOJ
Page 117 ~ Referral/Direct DOJ
Page 118 ~ Referral/Direct DOJ
Page 119 ~ Referral/Direct DOJ
Page 120 ~ Referral/Direct DOJ
Page 121 ~ Referral/Direct DOJ
Page 122 ~ Referral/Direct DOJ
Page 123 ~ Referral/Direct DOJ
Page 124 ~ Referral/Direct DOJ
Page 125 ~ Referral/Direct DOJ
Page 126 ~ Referral/Direct DOJ
Page 127 ~ Referral/Direct DOJ
Page 128 ~ Referral/Direct DOJ
Page 129 ~ Referral/Direct DOJ
Page 130 ~ Referral/Direct DOJ
Page 131 ~ Referral/Direct DOJ
Page 132 ~ Referral/Direct DOJ
Page 133 ~ Referral/Direct DOJ
Page 134 ~ Referral/Direct DOJ
Page 135 ~ Referral/Direct DOJ
Page 136 ~ Referral/Direct DOJ
Page 137 ~ Referral/Direct DOJ
Page 138 ~ Referral/Direct DOJ
Page 139 ~ Referral/Direct DOJ
Page 140 ~ Referral/Direct DOJ
Page 141 ~ Referral/Direct DOJ
Page 142 ~ Referral/Direct DOJ
Page 143 ~ Referral/Direct DOJ
Page 144 ~ Referral/Direct DOJ
Page 145 ~ Referral/Direct DOJ
Page 146 ~ Referral/Direct DOJ
Page 147 ~ Referral/Direct DOJ
Page 148 ~ Referral/Direct DOJ
Page 149 ~ Referral/Direct DOJ
Page 150 ~ Referral/Direct DOJ
Page 151 ~ Referral/Direct DOJ
Page 152 ~ Referral/Direct DOJ
Page 153 ~ Referral/Direct DOJ

Page 154 ~ Referral/Direct DOJ
Page 155 ~ Referral/Direct DOJ
Page 156 ~ Referral/Direct DOJ
Page 157 ~ Referral/Direct DOJ
Page 158 ~ Referral/Direct DOJ
Page 159 ~ Referral/Direct DOJ
Page 160 ~ Referral/Direct DOJ
Page 161 ~ Referral/Direct DOJ
Page 162 ~ Referral/Direct DOJ
Page 163 ~ Referral/Direct DOJ
Page 164 ~ Referral/Direct DOJ
Page 165 ~ Referral/Direct DOJ
Page 166 ~ Referral/Direct DOJ
Page 167 ~ Referral/Direct DOJ
Page 168 ~ Referral/Direct DOJ
Page 169 ~ Referral/Direct DOJ
Page 170 ~ Referral/Direct DOJ
Page 171 ~ Referral/Direct DOJ
Page 172 ~ Referral/Direct DOJ
Page 173 ~ Referral/Direct DOJ
Page 174 ~ Referral/Direct DOJ
Page 175 ~ Referral/Direct DOJ
Page 176 ~ Referral/Direct DOJ
Page 177 ~ Referral/Direct DOJ
Page 178 ~ Referral/Direct DOJ
Page 179 ~ Referral/Direct DOJ
Page 180 ~ Referral/Direct DOJ
Page 181 ~ Referral/Direct DOJ
Page 182 ~ Referral/Direct DOJ
Page 183 ~ Referral/Direct DOJ
Page 184 ~ Referral/Direct DOJ
Page 185 ~ Referral/Direct DOJ
Page 186 ~ Referral/Direct DOJ
Page 187 ~ Referral/Direct DOJ
Page 188 ~ Referral/Direct DOJ
Page 189 ~ Referral/Direct DOJ
Page 190 ~ Referral/Direct DOJ
Page 191 ~ Referral/Direct DOJ
Page 192 ~ Referral/Direct DOJ
Page 193 ~ Referral/Direct DOJ
Page 194 ~ Referral/Direct DOJ
Page 195 ~ Referral/Direct DOJ
Page 196 ~ Referral/Direct DOJ
Page 197 ~ Referral/Direct DOJ
Page 198 ~ Referral/Direct DOJ
Page 199 ~ Referral/Direct DOJ
Page 200 ~ Referral/Direct DOJ
Page 201 ~ Referral/Direct DOJ
Page 202 ~ Referral/Direct DOJ
Page 203 ~ Referral/Direct DOJ
Page 204 ~ Referral/Direct DOJ

Page 205 ~ Referral/Direct DOJ
Page 206 ~ Referral/Direct DOJ
Page 207 ~ Referral/Direct DOJ
Page 208 ~ Referral/Direct DOJ
Page 209 ~ Referral/Direct DOJ
Page 210 ~ Referral/Direct DOJ
Page 211 ~ Referral/Direct DOJ
Page 212 ~ Referral/Direct DOJ
Page 213 ~ Referral/Direct DOJ
Page 214 ~ Referral/Direct DOJ
Page 215 ~ Referral/Direct DOJ
Page 216 ~ Referral/Direct DOJ
Page 217 ~ Referral/Direct DOJ
Page 218 ~ Referral/Direct DOJ
Page 219 ~ Referral/Direct DOJ
Page 220 ~ Referral/Direct DOJ
Page 221 ~ Referral/Direct DOJ
Page 222 ~ Referral/Direct DOJ
Page 223 ~ Referral/Direct DOJ
Page 224 ~ Referral/Direct DOJ
Page 225 ~ Referral/Direct DOJ
Page 226 ~ Referral/Direct DOJ
Page 227 ~ Referral/Direct DOJ
Page 228 ~ Referral/Direct DOJ
Page 229 ~ Referral/Direct DOJ
Page 230 ~ Referral/Direct DOJ
Page 231 ~ Referral/Direct DOJ
Page 232 ~ Referral/Direct DOJ
Page 233 ~ Referral/Direct DOJ
Page 234 ~ Referral/Direct DOJ
Page 235 ~ Referral/Direct DOJ
Page 236 ~ Referral/Direct DOJ
Page 237 ~ Referral/Direct DOJ
Page 238 ~ Referral/Direct DOJ
Page 239 ~ Referral/Direct DOJ
Page 240 ~ Referral/Direct DOJ
Page 241 ~ Referral/Direct DOJ
Page 242 ~ Referral/Direct DOJ
Page 243 ~ Referral/Direct DOJ
Page 244 ~ Referral/Direct DOJ
Page 245 ~ Referral/Direct DOJ
Page 246 ~ Referral/Direct DOJ
Page 247 ~ Referral/Direct DOJ
Page 248 ~ Referral/Direct DOJ
Page 249 ~ Referral/Direct DOJ
Page 250 ~ Referral/Direct DOJ
Page 251 ~ Referral/Direct DOJ
Page 252 ~ Referral/Direct DOJ
Page 253 ~ Referral/Direct DOJ
Page 254 ~ Referral/Direct DOJ
Page 255 ~ Referral/Direct DOJ

Page 256 ~ Referral/Direct DOJ
Page 257 ~ Referral/Direct DOJ
Page 258 ~ Referral/Direct DOJ
Page 259 ~ Referral/Direct DOJ
Page 260 ~ Referral/Direct DOJ
Page 261 ~ Referral/Direct DOJ
Page 262 ~ Referral/Direct DOJ
Page 263 ~ Referral/Direct DOJ
Page 264 ~ Referral/Direct DOJ
Page 265 ~ Referral/Direct DOJ
Page 266 ~ Referral/Direct DOJ
Page 267 ~ Referral/Direct DOJ
Page 268 ~ Referral/Direct DOJ
Page 269 ~ Referral/Direct DOJ
Page 270 ~ Referral/Direct DOJ
Page 271 ~ Referral/Direct DOJ
Page 272 ~ Referral/Direct DOJ
Page 273 ~ Referral/Direct DOJ
Page 274 ~ Referral/Direct DOJ
Page 275 ~ Referral/Direct DOJ
Page 276 ~ Referral/Direct DOJ
Page 277 ~ Referral/Direct DOJ
Page 278 ~ Referral/Direct DOJ
Page 279 ~ Referral/Direct DOJ
Page 280 ~ Referral/Direct DOJ
Page 281 ~ Referral/Direct DOJ
Page 282 ~ Referral/Direct DOJ
Page 283 ~ Referral/Direct DOJ
Page 284 ~ Referral/Direct DOJ
Page 285 ~ Referral/Direct DOJ
Page 286 ~ Referral/Direct DOJ
Page 287 ~ Referral/Direct DOJ
Page 288 ~ Referral/Direct DOJ
Page 289 ~ Referral/Direct DOJ
Page 290 ~ Referral/Direct DOJ
Page 291 ~ Referral/Direct DOJ
Page 292 ~ Referral/Direct DOJ
Page 293 ~ Referral/Direct DOJ
Page 294 ~ Referral/Direct DOJ
Page 295 ~ Referral/Direct DOJ
Page 296 ~ Referral/Direct DOJ
Page 297 ~ Referral/Direct DOJ
Page 298 ~ Referral/Direct DOJ
Page 299 ~ Referral/Direct DOJ
Page 300 ~ Referral/Direct DOJ
Page 301 ~ Referral/Direct DOJ
Page 302 ~ Referral/Direct DOJ
Page 303 ~ Referral/Direct DOJ
Page 304 ~ Referral/Direct DOJ
Page 305 ~ Referral/Direct DOJ
Page 306 ~ Referral/Direct DOJ

Page 307 ~ Referral/Direct DOJ
Page 308 ~ Referral/Direct DOJ
Page 309 ~ Referral/Direct DOJ
Page 310 ~ Referral/Direct DOJ
Page 311 ~ Referral/Direct DOJ
Page 312 ~ Referral/Direct DOJ
Page 313 ~ Referral/Direct DOJ
Page 314 ~ Referral/Direct DOJ
Page 315 ~ Referral/Direct DOJ
Page 316 ~ Referral/Direct DOJ
Page 317 ~ Referral/Direct DOJ
Page 318 ~ Referral/Direct DOJ
Page 319 ~ Referral/Direct DOJ
Page 320 ~ Referral/Direct DOJ
Page 321 ~ Referral/Direct DOJ
Page 322 ~ Referral/Direct DOJ
Page 323 ~ Referral/Direct DOJ
Page 324 ~ Referral/Direct DOJ
Page 325 ~ Referral/Direct DOJ
Page 388 ~ Referral/Direct DOJ (pages 388-453)
Page 389 ~ Referral/Direct DOJ (pages 388-453)
Page 390 ~ Referral/Direct DOJ (pages 388-453)
Page 391 ~ Referral/Direct DOJ (pages 388-453)
Page 392 ~ Referral/Direct DOJ (pages 388-453)
Page 393 ~ Referral/Direct DOJ (pages 388-453)
Page 394 ~ Referral/Direct DOJ (pages 388-453)
Page 395 ~ Referral/Direct DOJ (pages 388-453)
Page 396 ~ Referral/Direct DOJ (pages 388-453)
Page 397 ~ Referral/Direct DOJ (pages 388-453)
Page 398 ~ Referral/Direct DOJ (pages 388-453)
Page 399 ~ Referral/Direct DOJ (pages 388-453)
Page 400 ~ Referral/Direct DOJ (pages 388-453)
Page 401 ~ Referral/Direct DOJ (pages 388-453)
Page 402 ~ Referral/Direct DOJ (pages 388-453)
Page 403 ~ Referral/Direct DOJ (pages 388-453)
Page 404 ~ Referral/Direct DOJ (pages 388-453)
Page 405 ~ Referral/Direct DOJ (pages 388-453)
Page 406 ~ Referral/Direct DOJ (pages 388-453)
Page 407 ~ Referral/Direct DOJ (pages 388-453)
Page 408 ~ Referral/Direct DOJ (pages 388-453)
Page 409 ~ Referral/Direct DOJ (pages 388-453)
Page 410 ~ Referral/Direct DOJ (pages 388-453)
Page 411 ~ Referral/Direct DOJ (pages 388-453)
Page 412 ~ Referral/Direct DOJ (pages 388-453)
Page 413 ~ Referral/Direct DOJ (pages 388-453)
Page 414 ~ Referral/Direct DOJ (pages 388-453)
Page 415 ~ Referral/Direct DOJ (pages 388-453)
Page 416 ~ Referral/Direct DOJ (pages 388-453)
Page 417 ~ Referral/Direct DOJ (pages 388-453)
Page 418 ~ Referral/Direct DOJ (pages 388-453)
Page 419 ~ Referral/Direct DOJ (pages 388-453)

Page 420 ~ Referral/Direct DOJ (pages 388-453)
Page 421 ~ Referral/Direct DOJ (pages 388-453)
Page 422 ~ Referral/Direct DOJ (pages 388-453)
Page 423 ~ Referral/Direct DOJ (pages 388-453)
Page 424 ~ Referral/Direct DOJ (pages 388-453)
Page 425 ~ Referral/Direct DOJ (pages 388-453)
Page 426 ~ Referral/Direct DOJ (pages 388-453)
Page 427 ~ Referral/Direct DOJ (pages 388-453)
Page 428 ~ Referral/Direct DOJ (pages 388-453)
Page 429 ~ Referral/Direct DOJ (pages 388-453)
Page 430 ~ Referral/Direct DOJ (pages 388-453)
Page 431 ~ Referral/Direct DOJ (pages 388-453)
Page 432 ~ Referral/Direct DOJ (pages 388-453)
Page 433 ~ Referral/Direct DOJ (pages 388-453)
Page 434 ~ Referral/Direct DOJ (pages 388-453)
Page 435 ~ Referral/Direct DOJ (pages 388-453)
Page 436 ~ Referral/Direct DOJ (pages 388-453)
Page 437 ~ Referral/Direct DOJ (pages 388-453)
Page 438 ~ Referral/Direct DOJ (pages 388-453)
Page 439 ~ Referral/Direct DOJ (pages 388-453)
Page 440 ~ Referral/Direct DOJ (pages 388-453)
Page 441 ~ Referral/Direct DOJ (pages 388-453)
Page 442 ~ Referral/Direct DOJ (pages 388-453)
Page 443 ~ Referral/Direct DOJ (pages 388-453)
Page 444 ~ Referral/Direct DOJ (pages 388-453)
Page 445 ~ Referral/Direct DOJ (pages 388-453)
Page 446 ~ Referral/Direct DOJ (pages 388-453)
Page 447 ~ Referral/Direct DOJ (pages 388-453)
Page 448 ~ Referral/Direct DOJ (pages 388-453)
Page 449 ~ Referral/Direct DOJ (pages 388-453)
Page 450 ~ Referral/Direct DOJ (pages 388-453)
Page 451 ~ Referral/Direct DOJ (pages 388-453)
Page 452 ~ Referral/Direct DOJ (pages 388-453)
Page 453 ~ Referral/Direct DOJ (pages 388-453)
Page 454 ~ Referral/Direct DOJ
Page 455 ~ Referral/Direct DOJ
Page 456 ~ Referral/Direct DOJ
Page 457 ~ Referral/Direct DOJ
Page 458 ~ Referral/Direct DOJ
Page 459 ~ Referral/Direct DOJ
Page 460 ~ Referral/Direct DOJ
Page 461 ~ Referral/Direct DOJ
Page 462 ~ Referral/Direct DOJ
Page 463 ~ Referral/Direct DOJ
Page 464 ~ Referral/Direct DOJ
Page 465 ~ Referral/Direct DOJ
Page 466 ~ Referral/Direct DOJ
Page 467 ~ Referral/Direct DOJ
Page 468 ~ Referral/Direct DOJ
Page 469 ~ Referral/Direct DOJ
Page 470 ~ Referral/Direct DOJ

Page 471 ~ Referral/Direct DOJ
Page 472 ~ Referral/Direct DOJ
Page 473 ~ Referral/Direct DOJ
Page 474 ~ Referral/Direct DOJ
Page 475 ~ Referral/Direct DOJ
Page 476 ~ Referral/Direct DOJ
Page 477 ~ Referral/Direct DOJ
Page 478 ~ Referral/Direct DOJ
Page 479 ~ Referral/Direct DOJ
Page 480 ~ Referral/Direct DOJ
Page 481 ~ Referral/Direct DOJ
Page 482 ~ Referral/Direct DOJ
Page 483 ~ Referral/Direct DOJ
Page 484 ~ Referral/Direct DOJ
Page 485 ~ Referral/Direct DOJ
Page 486 ~ Referral/Direct DOJ
Page 487 ~ Referral/Direct DOJ
Page 488 ~ Referral/Direct DOJ
Page 489 ~ Referral/Direct DOJ
Page 490 ~ Referral/Direct DOJ
Page 491 ~ Referral/Direct DOJ
Page 492 ~ Referral/Direct DOJ
Page 493 ~ Referral/Direct DOJ
Page 494 ~ Referral/Direct DOJ
Page 495 ~ Referral/Direct DOJ
Page 496 ~ Referral/Direct DOJ
Page 497 ~ Referral/Direct DOJ
Page 498 ~ Referral/Direct DOJ
Page 499 ~ Referral/Direct DOJ
Page 500 ~ Referral/Direct DOJ
Page 501 ~ Referral/Direct DOJ
Page 502 ~ Referral/Direct DOJ
Page 503 ~ Referral/Direct DOJ
Page 504 ~ Referral/Direct DOJ
Page 505 ~ Referral/Direct DOJ
Page 506 ~ Referral/Direct DOJ
Page 507 ~ Referral/Direct DOJ
Page 508 ~ Referral/Direct DOJ
Page 509 ~ Referral/Direct DOJ
Page 510 ~ Referral/Direct DOJ
Page 511 ~ Referral/Direct DOJ
Page 512 ~ Referral/Direct DOJ
Page 513 ~ Referral/Direct DOJ
Page 514 ~ Referral/Direct DOJ
Page 515 ~ Referral/Direct DOJ
Page 516 ~ Referral/Direct DOJ
Page 517 ~ Referral/Direct DOJ
Page 518 ~ Referral/Direct DOJ
Page 519 ~ Referral/Direct DOJ

From: KALISCH, ELENI P. (OCA) (FBI) b6
Sent: Monday, March 28, 2005 7:41 AM b7C
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act Examples

DATE: 09-19-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (c)
DECLASSIFY ON: 09-19-2030

Importance: High

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

05-CV-0845

~~SECRET~~
RECORD 66F[redacted]-A3035

b2
b7E

-----Original Message-----
From: [redacted] (FBI) b2
Sent: Saturday, March 26, 2005 10:09 AM b6
To: [redacted] (FBI); KALISCH, ELENI P. (OCA) (FBI) b7C
Cc: [redacted] (FBI) b7E
Subject: RE: Patriot Act Examples
Importance: High

~~SECRET~~
RECORD 66F-[redacted]-A3035 b2
b7E

(S)

[redacted] Eleni:

b1
Attached is the EC that addresses the USA PATRIOT ACT provisions that have been utilized in the [redacted] b2
Division. The case write-ups themselves are unclassified, however, the titles and file numbers are classified b6
~~SECRET~~ [redacted] Please advise if you would like additional b7C
clarification or information.

[redacted] b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Monday, March 21, 2005 10:01 AM b2
To: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI) b6
Subject: FW: Patriot Act Examples b7C
Importance: High b7E

UNCLASSIFIED
NON-RECORD

[redacted] let's put something together for this request. The deadline is this Friday! wdc
-----Original Message----- b6
From: KALISCH, ELENI P. (OCA) (FBI) b7C
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are

scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~SECRET~~

(Rev. 01-31-2003)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

DATE: 08-16-2005
CLASSIFIED BY 65179 DMH /JHF 05-CV-0845
REASON: 1.4 (C , D)
DECLASSIFY ON: 08-16-2030

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/25/2005

To: Office of Congressional Affairs **Attn:** AD Eleni P. Kalisch

From: [redacted] b2 , b7E
Squad 2
Contact: [redacted] b2 b6 b7C

Approved By: [redacted] b2 b6 b7C

Drafted By: [redacted]:djs b7E

Case ID #: (U) [redacted]-66F-A3035 (Pending)

Title: (U) USA PATRIOT ACT b2 , b7E
SUNSET PROVISIONS

Synopsis: (U) Case narratives provided as requested.

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Details: (U) As requested by the Office of Congressional Affairs, [redacted] is providing the following case narratives which describe investigations aided by provisions of the USA Patriot Act. b2 b7E

[redacted] b2 b6 b7A b7E

(U) Cited investigation was opened in [redacted] Upon further investigation it was determined that [redacted]

[redacted]

~~SECRET~~

To: Office of Congressional Affairs From: [redacted] b2
Re: (U) [redacted]-66F-A3035, 03/25/2005 b7E

[redacted] b6 b7A b7C

(U) Cited investigation has connections to cases operating in several other field divisions. This has required the coordination and sharing of information with these other offices at various times in the investigation. Based upon the international aspect of the investigation and the potential links to terrorism, cited investigation has been coordinated extensively with numerous foreign government law enforcement entities.

(U) A federal grand jury indicted [redacted]

[redacted] b2 b6 b7C b7A b7E

[redacted] was also arrested for [redacted]

(U) [redacted] b2 b7E

(U) Two sections of the USA PATRIOT Act were of particular use during cited investigation:

To: Office of Congressional Affairs From: [redacted] b2
Re: (U) [redacted]-66F-A3035, 03/25/2005 b7E

(U) Section 203(d): Information Sharing: Information derived from the Title III utilized in cited investigation was shared with foreign government law enforcement entities.

(U) Section 213: Delay in Search Warrant Notification: During the course of the investigation, on two instances, mail was searched and notification was delayed.

b6
b7A
b7C

(U) [redacted]

(U) Captioned investigation was partially predicated upon information [redacted] b6 b7A b7C

(U) [redacted] b6 b7A b7C

(U) Investigation to date has included the following investigative measures: [redacted] b2 b7A b7E

(U) [redacted] have been charged with [redacted]

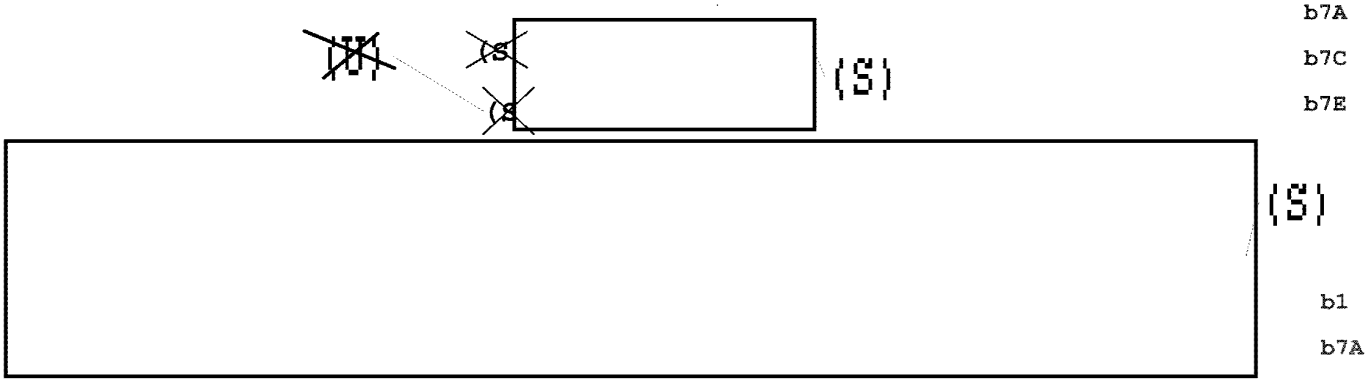
b6
b7A
b7C

(U) The following sections of the USA PATRIOT Act were utilized during the course of cited investigation:

(U) Section 203(d): Information Sharing: Information derived during the course of cited investigation was shared among other FBI field divisions conducting similar investigations. In addition, information obtained was also through the course of the investigation was

To: Office of Congressional Affairs From: [redacted] b2
Re: (U) [redacted]-66F-A3035, 03/25/2005 b7E

shared among the United States Intelligence Community and with foreign government law enforcement entities. b1 b2 b6 b7A b7C b7E

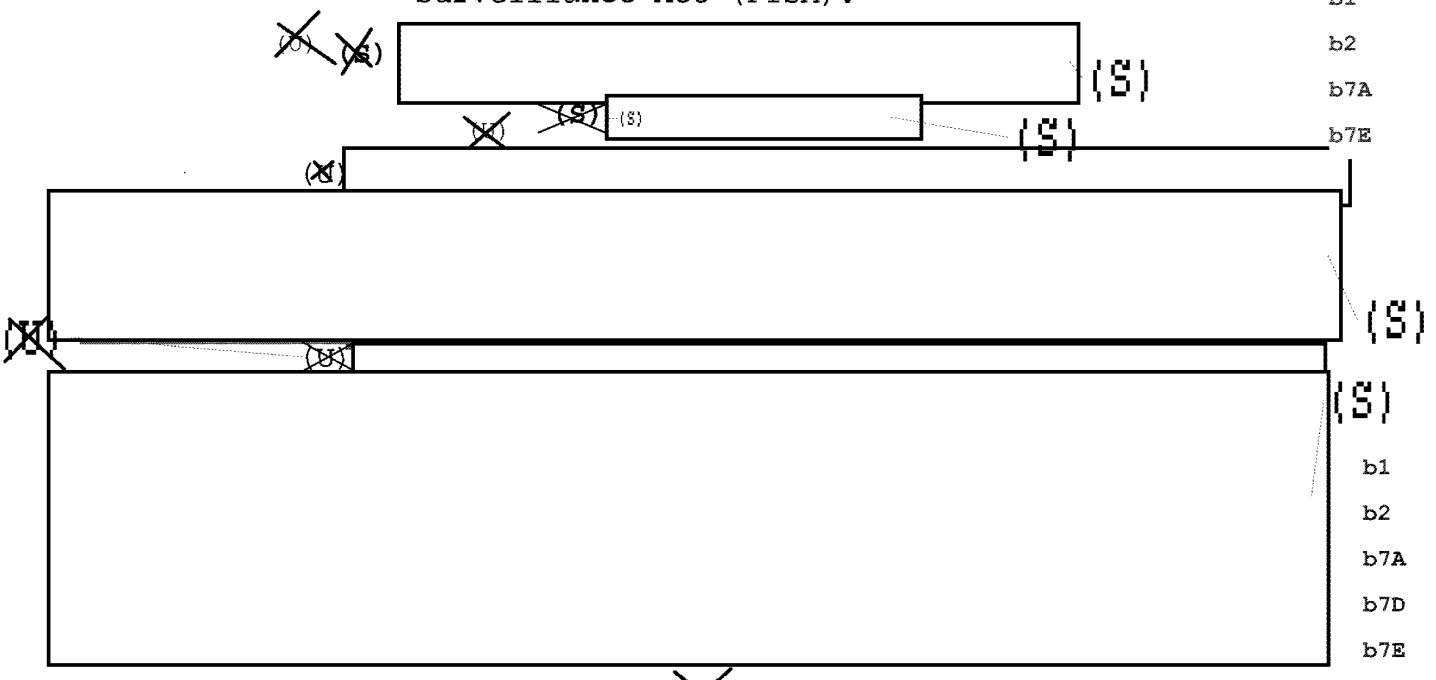


b1 b7A

(U) Cited matter is an on-going investigation.

(U) The following section of the USA PATRIOT Act have been utilized, to date, in cited investigation:

(U) Section 214: Utilization of Pen Registers/Trap and Trace Authority under the Foreign Intelligence Surveillance Act (FISA). b1 b2 b7A b7E



b1 b2 b7A b7D b7E

To: Office of Congressional Affairs From: [redacted] b2
Re: (U) [redacted]-66F-A3035, 03/25/2005 b7E

(U) The following sections of the USA PATRIOT Act have been utilized in cited investigation:

(U) Section 214(a): Pen Register/Trap and Trace Authority Under the Foreign Intelligence Surveillance Act (FISA). b2 b6 b7C b7E

(U) [redacted]
[redacted]- VICTIM;
IINI-[redacted]
PRODUCER/MANUFACTURER OF CHILD PORNOGRAPHY
305C[redacted]45511

(U) Investigation was initiated as a result of information provided by a local District Attorney's office which indicated that [redacted] had videotaped [redacted] year old [redacted] in sexually explicit poses. b6 b7C

(U) [redacted] b2 b7E

(U) The following section of the USA PATRIOT Act have been utilized in cited investigation:

(U) Section 220: Nationwide Service of Search Warrants for Electronic Evidence.

To: Office of Congressional Affairs From: [redacted] b2
Re: (U) [redacted]-66F-A3035, 03/25/2005 b7E

LEAD(s):

Set Lead 1: (Action)

(U) OFFICE OF CONGRESSIONAL AFFAIRS

AT WASHINGTON, DC

(U) Read and clear.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-10-2005 BY 65179 DMH/JHF

05-CV-0845

From: [redacted] (FBI)
Sent: Tuesday, March 29, 2005 4:22 PM
To: [redacted] (OCA) (FBI)
Cc: [redacted] (FBI)
Subject: FW: Patriot Act examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

[redacted]

See the below further explanation to your inquiry. Glad to be of service!

Tracey

-----Original Message-----
From: [redacted] (FBI)
Sent: Tuesday, March 29, 2005 10:15 AM
To: [redacted] (FBI)
Subject: RE: Patriot Act examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

[redacted]

After consultation with SA [redacted] regarding cited matter, SA [redacted] advised that two of the five listed reasons for delayed notification would have applied: a) sub-section 3: notification would reasonably be expected to result in destruction of, or tampering with, evidence; and b) sub-section 5: notification would reasonably be expected to cause serious jeopardy to an investigation or unduly delay a trial.

b6
b7C

I further inquired of SA [redacted] as to a more detailed explanation. SA [redacted] advised that cited investigation was originally covert. If delayed notification were not available, the target of this investigation would have obtained knowledge of the investigation. This would have destroyed the covert nature of this investigation and would reasonably have caused the main target to destroy, and/or tamper with evidence.

-----Original Message-----
From: [redacted] (FBI)
Sent: Tuesday, March 29, 2005 7:29 AM
To: [redacted] (OCA) (FBI); [redacted] (FBI)
Subject: FW: Patriot Act examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

[redacted]

Can you please reach out to the [redacted] Case Agent and determine the answer to [redacted] question?

b2
b6
b7C
b7E

Thank you,

[redacted]

-----Original Message-----
From: [redacted] (OCA) (FBI)

b6
b7C

b2
b6
b7C
b7E

Sent: Monday, March 28, 2005 11:44 AM
To: [redacted] (FBI)
Subject: Patriot Act examples

UNCLASSIFIED
NON-RECORD

[redacted] I already love having you in [redacted] thanks for the great Patriot Act examples in a very user-friendly format!!
I have 1 quick question: In your first example, you reference using §213 (delayed notice). The statute requires the govt to cite to one of five specific circumstances in requesting delayed notice. The five circumstances are set forth below. Can you let me know which [redacted] relied on in seeking the delayed notice warrant? Thanks as always!

b2
b6
b7C
b7E

****

Pursuant to section 213, prosecutors can seek a judge's approval to delay notification by making a showing that if notification were made contemporaneous to the search, there is reasonable cause to believe one of the following might occur:

1. notification would reasonably endanger the life or physical safety of an individual;
2. notification would reasonably be expected to cause flight from prosecution;
3. notification would reasonably be expected to result in destruction of, or tampering with, evidence;
4. notification would reasonably result in intimidation of potential witnesses; or
5. notification would reasonably be expected to cause serious jeopardy to an investigation or unduly delay a trial.

****

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

b6
b7C

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 24, 2005 6:21 PM
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples

DATE: 12-27-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-27-2030

UNCLASSIFIED
RECORD 00

05-cv-0845

-----Original Message-----
From: [redacted](FBI)
Sent: Thursday, March 24, 2005 6:12 PM
To: [redacted](FBI); KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI)
Subject: RE: Patriot Act Examples

b2
b6
b7C
b7E

UNCLASSIFIED
RECORD 00

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Eleni,

b6
b7C

SAC [redacted] asked me to forward this to you. It was prepared by our [redacted] (in conjunction with all Program coordinators and managers) [redacted] will be our POC for this initiaitive should you need any additional information

Thanks

b6
b7C

[redacted] SSA

---

b2
b7E

The following is provided in response to your request for input on the sunset provisions of the PATRIOT Act. The three sunset provisions that the [redacted] Division has utilized and benefitted from the most are the information sharing, changes to primary purpose standard for FISA, and the nationwide search warrants.

The information sharing sunset provisions of the PATRIOT Act combined with the changes to the primary purpose standard for FISA have probably been the most vital changes brought about in the sunset provisions of the PATRIOT Act.. Together, these provisions have allowed us to utilize the criminal tools and expertise of the US Attorneys Office in coordination with our intelligence tools to neutralize international terrorism targets. In [redacted] this has worked very well as the US Attorneys office representative working with our JTTF has been a key partner in devising strategy to attack terrorist threats. This division has numerous IT investigations where criminal investigative tools such as federal grand jury subpoenas have been utilized. There have also been several instances where we have obtained emergency FISAs where we discussed both criminal and intelligence objectives right from the

b2
b7E

beginning of the investigation. As a general matter, this coordination occurs on a daily basis in a manner that would have been much more difficult if not impossible before the enactment of these sunset provisions of the PATRIOT Act. This has increased our efficiency in our attempts to immediately neutralize Islamic extremists. It is the opinion of a [redacted] SSA that without the ability to utilize both criminal and intelligence tools in a coordinated manner it would be nearly impossible to neutralize terrorist targets. b2 b7E

(S) (S)

The other sunset provision that has had a very significant impact on [redacted] Division cases is the nationwide search warrant. [redacted] has utilized this approximately [redacted] times in connection with its [redacted] investigation, and on [redacted] occasions in connection with a computer intrusion case (288A-[redacted]103932). [redacted] experience in the use of the nationwide search warrants to obtain e-mail from ISPs has shown that they significantly reduce the time it takes to obtain contents of e-mail accounts, and results in a much more efficient use of agent investigative resources. This reduction in time can allow us to obtain information that would otherwise be lost because of [redacted] It is foreseeable that the time saved obtaining information through the use of nationwide search warrants could have other benefits. While we can not state with certainty that up to this point the use of a nationwide search warrant definitely prevented an act of child sexual exploitation, because of the reduction in time it takes to obtain e-mail information through the use of a nationwide warrant, it is very conceivable that the use of a nationwide warrant in connection with the Innocent Images investigation could prevent such an act of child exploitation at some point in the future. b1 b2 b7E

Regarding the other sunset provisions of the PATRIOT Act, while we have not had many specific instances of implementing their use, it is certainly foreseeable that the need for their use could come up. The sunset provision requiring the use of a FISA business court order for obtaining business records, while certainly better than the previous law, is overly burdensome, and should be changed to allow access to such records with an administrative subpoena. As the legislation about to sunset is written, the FISA business record provision could be very useful, but has been under utilized because of the length of time it took to get the orders in the past. I believe we may see an increase in the use of FISA court orders for business records as agents become aware that the FBI may obtain these directly from the court. Up until recently we had to go through DOJ to obtain these and, while I do not have any specific instances of when we tried to get one, I can tell you that when the DOJ had to obtain these orders, the impression of the field was that it would take months to get one of these orders. We had an instance a couple of years ago when we wanted to obtain [redacted] records in an expedited manner and didn't even bother because by the time OIPR got the order we would not need the records any more. If I recall correctly, we were lucky because a persuasive agent obtained them with consent. Now I believe the FBI will be obtaining these directly from the FISA court and it is anticipated that it will take much less time to get an order. We have tried to get the word out to use these orders but up to now have not had much of a response, in part because of the general knowledge of the previous DOJ institutional inertia. b2 b7E

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the

Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 11:27 AM
To: [redacted] (OCA) (FBI)
Subject: FW: Sunset examples

b6
b7C

DATE: 09-19-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (c)
DECLASSIFY ON: 09-19-2030

05-CV-0845

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Wow! [redacted] is all over it!

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Friday, March 25, 2005 11:25 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted] (FBI)
Subject: Sunset examples

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Eleni,

Below please find the requested information re sunset provisions.

Section 214 - [redacted] successfully utilized FISA pens [redacted] (S) which provided locally significant intelligence concerning international terrorism.

b1
b2
b7E

Section 203/218 - [redacted] successfully provided intel gained via FISA coverage to criminal agents to support an ongoing criminal investigation into material support of terrorism.

SA [redacted]
[redacted] DIVISION
SQUAD CT-1
[redacted]

b2
b6
b7C
b7E

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SENSITIVE BUT UNCLASSIFIED~~

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 24, 2005 4:43 PM
To: [redacted](OCA) (FBI) b6
Subject: FW: Patriot Act b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-10-2005 BY 65179 DMH/JHF

05-CV-0845

-----Original Message-----
From: [redacted](FBI) b2
Sent: Thursday, March 24, 2005 4:41 PM b7E
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: Patriot Act

UNCLASSIFIED
NON-RECORD

Elini:

Please see the attached Patriot Act example from the [redacted] Division. I just arrived as the Counterterrorism ASAC so my personal knowledge of the division is limited. Should this not suffice, or you need additional information, please don't hesitate to call [redacted] or email me. b2 b7E

Thanks.

[redacted] b2 b7E

UNCLASSIFIED

UNCLASSIFIED

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Tuesday, March 29, 2005 8:54 AM
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples

b6
b7C

UNCLASSIFIED
NON-RECORD

05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-10-2005 BY 65179 DMH/JHF

-----Original Message-----
From: [redacted](FBI)
Sent: Tuesday, March 29, 2005 8:27 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted]OCA) (FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI)
Subject: Patriot Act Examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Ms. Kalisch:

b2

SAC [redacted] requested that I forward to you some examples of positive uses of the Patriot Act by [redacted] Division CT Squads. The below is provided for your consideration:

b7E

Section 218 permitted the full coordination between intelligence and law enforcement. Previously, FISA could only be used when foreign intelligence was the "primary purpose" of an investigation, but now it can be used whenever foreign intelligence is a significant purpose of an investigation. Now we can take criminal information derived from FISA and share/use in a criminal proceeding. We have used this provision in the [redacted] investigation in which three [redacted] leaders were indicted in [redacted] and charged with RICO, Material Support, and Obstruction of Justice in conjunction with [redacted] criminal terrorist activities.

b2
b6
b7C
b7E

Section 505 allowed the SAC to approve National Security Letters (NSL). Prior to the PATRIOT Act they had to be approved at FBIHQ and would take months to get them. As you well know, we send NSLs for approval quite often, and the turnaround has been significantly improved.

In a[redacted] case, subject [redacted]

b2
b6
b7A

I hope this is useful, and if you have any questions, please don't hesitate to call.

b7E

[redacted] ASAC [redacted] CT Program, [redacted]

b2
b7E

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

PATRIOT ACT PROVISIONS:
COUNTERINTELLIGENCE DIVISION: EAST ASIA SECTION: CD-3D

INFORMATION SHARING:

FBI INITIATIVES:

[redacted] (S)

b1
b2
b7E

[redacted] (S)

b1
b2
b7E

FBI INVESTIGATIONS:

[redacted] (S)

b1
b2
b7E

~~SECRET~~

(S)

b1
b2
b7E

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Tuesday, March 29, 2005 8:54 AM
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act Examples

b6
b7C

DATE: 12-03-2005
CLASSIFIED BY 61578TMW/AP/DFW
REASON: 1.4 ((C))S-CP-0845)
DECLASSIFY ON: 12-03-2030

Importance: High

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: BEREZNAY, TIMOTHY D. (CD) (FBI)
Sent: Tuesday, March 29, 2005 8:27 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

-----Original Message-----
From: DESLAURIERS, RICHARD (CD) (FBI)
Sent: Thursday, March 24, 2005 12:12 PM
To: BEREZNAY, TIMOTHY D. (CD) (FBI)
Cc: [redacted] (CD) (FBI)
Subject: RE: Patriot Act Examples
Importance: High

b6
b7C

b1
b2
b7E

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Tim:

[redacted] (S)

[redacted] (S)

[redacted] (S)

[redacted] (S)

SECRET

b1
b2
(S) b7E

I hope this sensitive but unclassified CD-2 response assists OCA efforts to renew the Patriot Act "sunset" provisions, as they pertain to Section 214. Rick

Richard DesLauriers
Section Chief, Global Section (CD-2)
Counterintelligence Division

b2

-----Original Message-----
From: BEREZNAY, TIMOTHY D. (CD) (FBI)
Sent: Monday, March 21, 2005 10:19 AM
To: DONNER, MICHAEL A. (CD) (FBI); DESLAURIERS, RICHARD (CD) (FBI); GUERIN, RONALD T. (CD) (FBI); FAVREAU, KEVIN (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

Pls canvas your troops and provide examples to me by noon Thursday.
-----Original Message-----
From: SZADY, DAVID (CD) (FBI)
Sent: Monday, March 21, 2005 8:01 AM
To: BEREZNAY, TIMOTHY D. (CD) (FBI); ANDRESS, BEVERLY (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

b2

I know we have wxamples such as Rudy's b7E
-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website

b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

b6
b7C

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Tuesday, March 29, 2005 8:55 AM
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

05-CV-0845

DATE: 12-29-2005
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-29-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: BEREZNAY, TIMOTHY D. (CD) (FBI)
Sent: Tuesday, March 29, 2005 8:33 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: FW: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: DONNER, MICHAEL A. (CD) (FBI)
Sent: Wednesday, March 23, 2005 1:48 PM
To: BEREZNAY, TIMOTHY D. (CD) (FBI)
Cc: [redacted] (CD) (FBI); SULLIVAN, DONALD T. (CD) (FBI); [redacted] (CD) (FBI)
Subject: FW: Patriot Act Examples

b6
b7C

UNCLASSIFIED
NON-RECORD

Tim..attached are two examples identified by the A unit concerning the benefits of the Patriot Act supporting CI investigations.

Donner

[redacted].thanks for the input.
-----Original Message-----
From: [redacted] (CD) (FBI)
Sent: Wednesday, March 23, 2005 12:51 PM
To: DONNER, MICHAEL A. (CD) (FBI)
Cc: [redacted] (CD) (FBI); [redacted] (CD) (FBI)
Subject: RE: Patriot Act Examples

b6
b7C

UNCLASSIFIED
NON-RECORD

Mike - Here are two examples in support of continuning or reauthorization of the roving authority and the FISA pen register and trap and trace section:

(S)

EX 1: In 2004, shortly after the roving authority was implemented, an [redacted]

b1
b2
b7E

SECRET

[redacted] This b1
would not have been possible without the roving authority. b2

(S) EX 2: The Pen Register and Trap and Trace Section of the Patriot Act allowed an investigator in an b7E
[redacted] (S)
(S)

b6
Regards, dm b7C

-----Original Message-----
From: [redacted] (CD) (FBI)
Sent: Monday, March 21, 2005 11:15 AM
To: [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD)(FBI); [redacted] (CD)(FBI); [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD)(FBI); [redacted] (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All-

Please review and send any examples to [redacted] acting UC on Wed). [redacted] - please combine responses and send them up to Mike Donner. b6 b7C

thanks

[redacted]

-----Original Message-----
From: DONNER, MICHAEL A. (CD) (FBI)
Sent: Monday, March 21, 2005 11:13 AM
To: [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD) (FBI); [redacted] (CD) (FBI)
Cc: [redacted] (CD) (FBI) b6
Subject: FW: Patriot Act Examples b7C
Importance: High

UNCLASSIFIED
NON-RECORD

All..attached provided from DAD Bereznay concerning Patriot Act..kindly respond to me by noon Wednesday with any examples ..unclassified..in support of continuning or reauthorization of certain provisions.

Donner
-----Original Message-----
From: BEREZNAY, TIMOTHY D. (CD) (FBI)

~~SECRET~~

Sent: Monday, March 21, 2005 10:19 AM
To: DONNER, MICHAEL A. (CD) (FBI); DESLAURIERS, RICHARD (CD) (FBI); GUERIN, RONALD T. (CD) (FBI); FAVREAU, KEVIN (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

Pls canvas your troops and provide examples to me by noon Thursday.
-----Original Message-----
From: SZADY, DAVID (CD) (FBI)
Sent: Monday, March 21, 2005 8:01 AM
To: BEREZNAY, TIMOTHY D. (CD) (FBI); ANDRESS, BEVERLY (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

I know we have wxamples such as Rudy's [redacted] b2 b7E
-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

SECRET

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED SECRET

UNCLASSIFIED

From: [redacted](CID) (FBI) b6
Sent: Thursday, March 24, 2005 9:13 AM b7C
To: [redacted]OCA) (FBI)
Cc: WILLIAMS, WK (CID) (FBI); GREGORSKI, CHARLES C. (CID) (FBI); BURRUS, JAMES H. (CID) (FBI); CUNNINGHAM, CHARLES J. (CID) (FBI); [redacted](CID) (FBI); [redacted] CID) (FBI); MINES, MICHAEL C. (CID)(FBI); [redacted] (CID) (FBI); PIERCE, D. S. (CID) (FBI); ROONEY, CHARLES J. (CID) (FBI); SWECKER, CHRIS (CID) (FBI); METZ, THOMAS R. (CID) (FBI); SIEGLE, DEREK M. (CID) (FBI); JACKSON, JOHNNIE E. (CID) (FBI); [redacted] CID) (FBI); KALISCH, ELENI P. (OCA) (FBI)
Subject: RE: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

[redacted] b6
b7C
referred me to you for guidance on the requested Patriot Act Examples for the Sunset provisions - CID has numerous examples to support the continued need for easy information sharing between, CT, CI and Criminal. CID previously prepared a list of cases showing this interrelationship for a response to the WMD commission. This slightly reworked list is attached - it has been somewhat sanitized but still contains some very sensitive information - classified or unclassified.
I wanted you to take a look at it because I am concerned the more sanitized the information, the less weight it carries in support of our arguments.

Thanks x [redacted] b2
b6
b7C

-----Original Message-----
From: SWECKER, CHRIS (CID) (FBI)
Sent: Sunday, March 20, 2005 5:21 PM
To: [redacted]CID) (FBI)
Cc: WILLIAMS, WK (CID) (FBI); BURRUS, JAMES H. (CID) (FBI); [redacted](CID) (FBI); CUNNINGHAM, CHARLES J. (CID) (FBI); [redacted](CID) (FBI); [redacted](SE) (FBI); MINES, MICHAEL C. (CID)(FBI); [redacted] CID) (FBI); PIERCE, D. S. (CID) (FBI); ROONEY, CHARLES J. (CID) (FBI); [redacted](CID) (FBI) b6 b7C
Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

[redacted] will coordinate our response. Pls canvass for examples. b6

Chris Swecker b7C

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are

scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

PATRIOT ACT
SUNSET PROVISIONS

CID EXAMPLES OF THE NEED FOR PATRIOT ACT SECTIONS 203 AND 218 (INFORMATION SHARING)

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist and foreign intelligence organizations and acts are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some of these examples which support the need for continued information sharing between criminal, counterterrorism and counterintelligence efforts are set forth below:

A. Transnational Criminal Enterprises

b2
b7A
b7E

1. [redacted]

b2
b7A
b7E

[redacted]

Ongoing.

2. [redacted] b2 , b7A, b7E

[redacted]

b2
b7A
b7E

[redacted] Ongoing.

3. Alien Smuggling

[redacted]

b2
b7E

The following are examples of criminal intelligence developed and disseminated on alien smuggling matters:

b2
b6
b7A
b7E

a. [redacted] FBI [redacted]

[redacted]

b. [redacted] FBI [redacted]

[redacted]

b2
b7A
b7E

c. [redacted]

[redacted]

d. [redacted] FBI [redacted]

[redacted]

(S)

b1
b2
b6
b7A
b7C
b7D
b7E

[redacted]

4. [redacted]

[redacted]

5. [redacted]

[redacted]

b2
b6
b7A
b7C
b7E

[redacted] Ongoing.

6. [redacted] b2 b7E

[redacted]

7. [redacted]

[redacted] b2 b7A b7E

the arrest, indictment and subsequent deportation of the subjects from Hong Kong to [redacted]
The charges included narcotics violations and providing material support to Al Qaeda.

8. [redacted]

[redacted] b2 b6 b7A b7C b7E

Ongoing.

9. [redacted]

[redacted] b2 b7A b7E

10. [redacted] b2 ,b7A, b7E

[redacted]

b2 b7E

b2
b6
b7A
b7C
b7E

B. Americas Criminal Enterprises (drugs/gangs/major theft enterprises)

1. [redacted] (199M-[redacted]-280706) (281H-[redacted]-281341)
[redacted]

Investigation began as a Pentbomb lead concerning [redacted] in [redacted] was identified and determined to be a Taliban/Al Qaeda associate. He was a financial contributor to the Taliban and [redacted] where drug trafficking took place. He filed a fraudulent death claim for [redacted] with an insurance company and was convicted of mail fraud. One of his employees was located in [redacted] and deported after a drug conviction.

2. [redacted]

b2
b7A
b7E

[redacted]

3. [redacted]

b2
b6
b7A
b7C
b7E

[redacted] Ongoing

4. [redacted]

[redacted]. Ongoing.

b2
b7A
b7E

5. [redacted]

[redacted] Ongoing.

b2
b6
b7A
b7C
b7E

b2
b7A
b7E

C. White Collar Crimes

1. Unlawful Redemption [ ] 265C[ ]-42132, [ ] 265F-[ ]-282769)

[ ] b2 b6 b7A b7E

Ongoing.

b2 , b7A, b7E

2. [ ]

[ ] b2 b6 b7A b7C b7E

3 [ ] (272-[ ]97082) b2 , b6, b7C, b7E

A drug/money laundering investigation identified subjects in Colombia, Spain, England and U.S., including a subject affiliated with the United Self-Defense Forces of Colombia (AUC), which is a recognized Foreign Terrorist Organization. Subject wants to purchase a bank in the U.S. to facilitate laundering of drug proceeds. Ongoing.

4. [ ] b2 , b7A, b7E

[ ] b2 b7A b7E

[ ] Ongoing

5. Express Cleaners (272D-[ ]-40807) b2 b7E

Investigation determined subjects were in position to launder millions through a location outside the U.S. through Lebanese and Saudi Arabian banks. The money would be returned to U.S. "clean" for a 20% fee. Two subjects identified had links to terrorists or terrorist activities.

b2 , b6, b7A, b7C, b7E

6. [ ]

[ ] b2 b7A b7E

b2 , b6, b7C, b7C, b7E

7. [redacted]

[redacted]

b2
b6
b7A
b7C
b7E

8. [redacted] b2 , b6, b7C, b7E

[redacted]

b2
b7A
b7E

[redacted] Ongoing. b2 , b6, b7A, b7C, b7E

9. [redacted]

[redacted]

b1
(S) b2
b7A
b7E

10. [redacted] b2 , b6, b7A, b7C, b7E

[redacted]

b2
b6
b7A
b7C
b7E

[redacted] Ongoing.

11. [redacted] b2 , b6, b7A, b7C, b7E

[redacted]

b2
b7A
b7E

12. [redacted] b6 b7A, b7C

[redacted]

b6
b7A
b7C

b2
b7A
b7D
b7E

D. Public Corruption

1. b2 , b7A, b7E

b2
b7A
b7D
b7E

Ongoing.

2. b7A

b2
b7A
b7E

3. (265B- -42623

b2
b6
b7A
b7C
b7E

b2 Ongoing.
b6
b7A
b7C
b7E

E. Civil Rights

1. Human Trafficking Investigations

Target organizations who traffic in aliens to be used as domestic servants, prostitutes and migrant workers. Investigations also develop foreign intelligence information.

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 9:15 AM
To: [redacted](OCA) (FBI)
Subject: FW: patriot act provisions survey

b6
b7C

UNCLASSIFIED
RECORD 1a-c545

05-CV-0845

-----Original Message-----
From: [redacted](FBI)
Sent: Friday, March 25, 2005 9:09 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: RE: patriot act provisions survey

b2
b6
b7C
b7E

UNCLASSIFIED
RECORD 1a-c545

Based on an office-wide canvas, the only example to provide from the [redacted] Division relates to Section 206 of the PATRIOT ACT regarding roving FISA surveillance [redacted]

b2
b6
b7A
b7C
b7E

[redacted] is on AL until April 4. POC at [redacted] In the interim is [redacted]

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 8:35 AM
To: [redacted](FBI)
Subject: RE: patriot act provisions survey

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Here is the tasking e-mail. Informal e-mail responses were requested. Thanks.

-----Original Message-----
From: [redacted](FBI)
Sent: Friday, March 25, 2005 8:00 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: patriot act provisions survey

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Hi... I'm preparing [redacted] response to your inquiry and will submit an email regarding same, but was wondering if there is an EC setting out a lead regarding this inquiry. I can prepare an EC and email it to you as an attachment for [redacted] response, or simply send an email. Please let me know if you'd like a formal EC in response. Thank you!

b2
b7E

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 24, 2005 4:07 PM
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples

b6
b7C

DATE: 09-19-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (c)
DECLASSIFY ON: 09-19-2030

~~UNCLASSIFIED~~
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

05-CV-0845

-----Original Message-----
From: [redacted](FBI)
Sent: Thursday, March 24, 2005 3:58 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted]FBI); [redacted]FBI)
Subject: RE: Patriot Act Examples

b2
b7E

~~UNCLASSIFIED~~
NON-RECORD

Ms. Kalisch:

The following is information I was able to gather from our CT squad in [redacted] am still waiting for information from our CT squad in [redacted] but they are all working a time critical investigation this week and I doubt I will have any additional information from them before COB 3/25. When I get information from this squad I will forward it.

b2
b7E

[redacted]

(S)

b1
b2
b7A
b7E

The undersigned is the point of contact for the [redacted] Division for any follow-up questions.

[redacted]

b2
b6
b7C
b7E

~~SECRET~~

b2
b7E

-----Original Message-----
From [redacted](FBI)
Sent: Thursday, March 17, 2005 2:21 PM
To: [redacted](FBI)
Cc: [redacted](FBI)
Subject: FW: Patriot Act Examples
Importance: High

b2
b6
b7C
b7E

~~UNCLASSIFIED~~

NON-RECORD

b6
b7C

[redacted] Please handle this. [redacted]
-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted]

b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED ~~SECRET~~

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

Cyber Division - Patriot Act Examples

b2
b5
b7D
b7E

b2
b7A
b7D
b7E

From: [redacted](FBI) b2
Sent: Wednesday, March 30, 2005 7:52 AM b6
To: [redacted]OCA) (FBI) b7C
Cc: [redacted](FBI); [redacted](FBI); [redacted] b7E
[redacted](FBI)
Subject: FW: SPECIFIC EXAMPLES ON THE PATRIOT ACT PROVISION - Voluntary Disclosure by ISP

UNCLASSIFIED
NON-RECORD

DATE: 12-29-2005
CLASSIFIED BY 65179dmh/baw
REASON: 1.4 (c)
DECLASSIFY ON: 12-29-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]

[redacted] SA [redacted] was notified by the USAO that the order was signed to unseal the case by the Magistrate Judge regarding the example on the Voluntary Disclosure by an ISP. Do you need a copy of the Order? Also, please notify me if [redacted] can provide you with any other data. b2 b6 b7C b7E

Thanks!
[redacted]

-----Original Message-----
From: [redacted](FBI) b2 b6 b7C b7E
Sent: Tuesday, March 29, 2005 4:32 PM
To: [redacted](FBI)
Cc: [redacted]FBI)
Subject: RE: SPECIFIC EXAMPLES ON THE PATRIOT ACT PROVISION

UNCLASSIFIED
NON-RECORD

[redacted]

I just got a call from the USAO, the order has been signed and they will forward a copy to me via the mail. b6 b7C

[redacted]

-----Original Message-----
From: [redacted](FBI) b2 b6 b7C b7E
Sent: Tuesday, March 29, 2005 10:46 AM
To: [redacted]FBI); [redacted]FBI)
Cc: [redacted]FBI)
Subject: RE: SPECIFIC EXAMPLES ON THE PATRIOT ACT PROVISION

UNCLASSIFIED
NON-RECORD

[redacted]

Please confirm to me by email regarding the order filed to unseal the case by which information may be released. Congressional Affairs is waiting on your response. b6 b7C

Thanks.
[redacted]

SECRET

-----Original Message-----
From: [redacted] FBI)
Sent: Monday, March 28, 2005 5:08 PM
To: [redacted] (FBI); [redacted] FBI)
Subject: RE: SPECIFIC EXAMPLES ON THE PATRIOT ACT PROVISION

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

[redacted] I spoke with [redacted] regarding this matter and she stated that the case were under seal. However, as the case was being closed she felt there would not be a problem unsealing the matter. She indicated she would submit the order to unseal the matter today (3/29/2005).

Additional information (S)

[redacted] (S)

(S)

b1
b2
b6
b7C
b7D
b7E

Let me know if this is all you need.

[redacted]

b2
b6
b7C

P.S. I am at headquarters, the only way to get a hold of me is via my pager [redacted]

-----Original Message-----
From: [redacted] (FBI)
Sent: Monday, March 28, 2005 12:48 PM
To: [redacted] FBI)
Cc: [redacted] (FBI); [redacted] FBI)
Subject: RE: SPECIFIC EXAMPLES ON THE PATRIOT ACT PROVISION

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

The public disclosure is fine with me but do no refer to the specific case file

SECRET

because this case is in support of a Group 1. (S)

(S)

SSA
Cyber Squad

-----Original Message----- b2
From: FBI) b6
Sent: Friday, March 25, 2005 3:12 PM
To: (FBI); (FBI) b7C
Cc: GONZALEZ, GUADALUPE (FBI); COWARD, RODERICK W FBI); b7E
FBI)
Subject: SPECIFIC EXAMPLES ON THE PATRIOT ACT PROVISION
Importance: High

UNCLASSIFIED b6
NON-RECORD b7C

In 2004, you reported the below information regarding the Patriot Act Provisions. HQ, Office of Congressional Affairs, is requesting the following:

* On the §212 case - this is a great example and factually distinct from most that we have for this provision. What's the status of this investigation and the classification of the information contained in this narrative? Can this info be used in a public statement? If not, is there anything we can say publically?

Please respond by email to deadline: COB March 28, 2005. The Director will be testifying before Congress on the information you provide (per Office of Congressional Affairs). b6 b7C

Thank you

SECRET

1.

-Voluntary Disclosure by ISP (18 USC §212) (S)	OCT 10/22/04 FBI received a lead from the legat in regarding an internet threat agains people if they did not pull their t out of Iraq. The web site hosting this bulletin b was hosted at , a based interne service provider, contacted regarding this matter and they provided us acce the electronic content of the server in order to identify the source of the threatening post. (S)

b1
b2
b7D
b7E

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 08-23-2005
CLASSIFIED BY 65179 DMH / JHF
REASON: 1.4 (C , D)
DECLASSIFY ON: 08-23-2030

05-CV-0845

[redacted] DIVISION REPORT

TRACKING THE USE OF THE PATRIOT ACT PROVISIONS

b2
b6
b7C
b7E

Paralegal Specialis[redacted]

b1
b2
b7A
b7E

(S)

~~SECRET~~

X

b1
b2
b7A
b7E

(S)

(S)

X

X

X

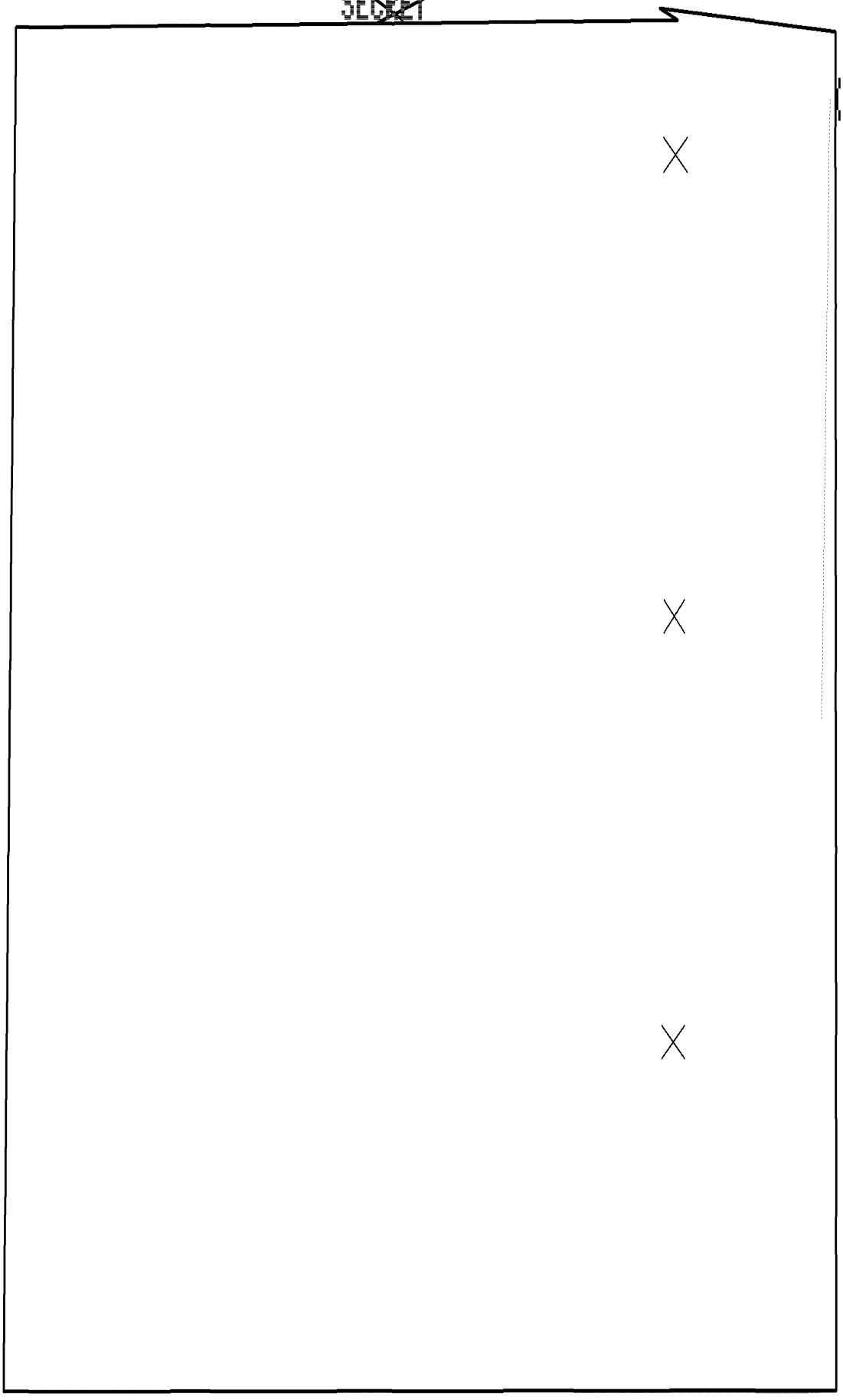
b1

b2

b7A

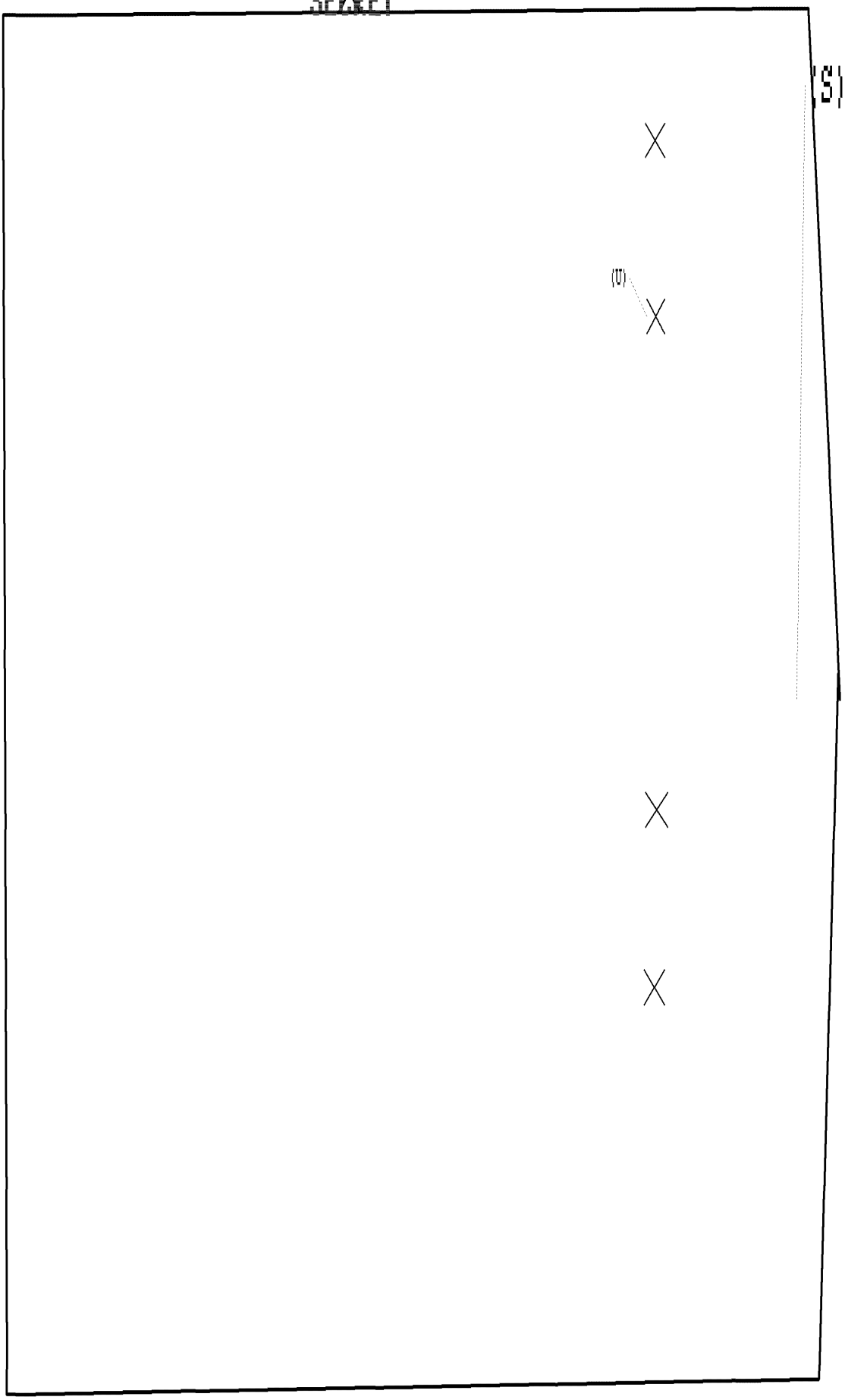
b7E

(S)

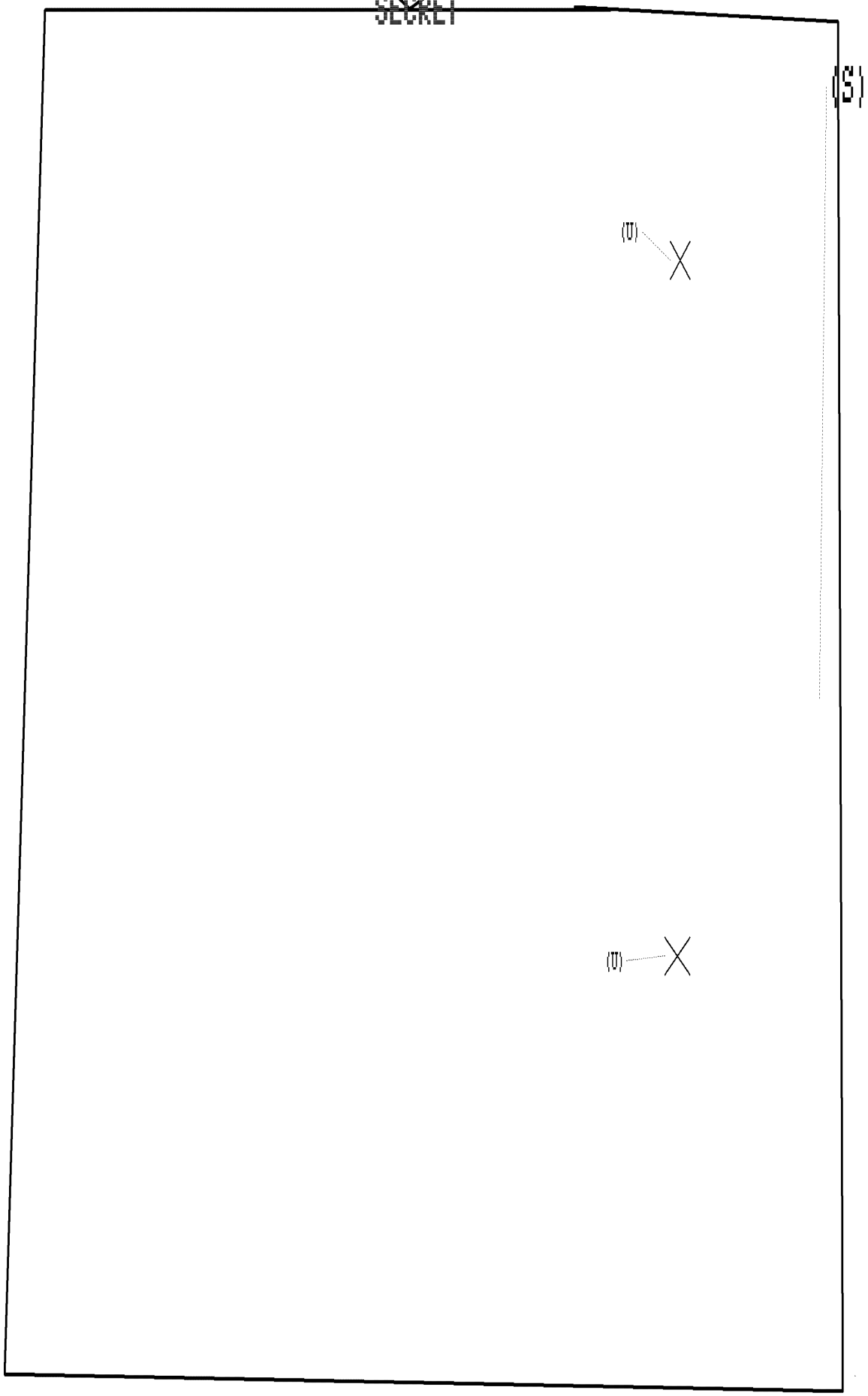


b1
b2
b7A
b7E

(S)

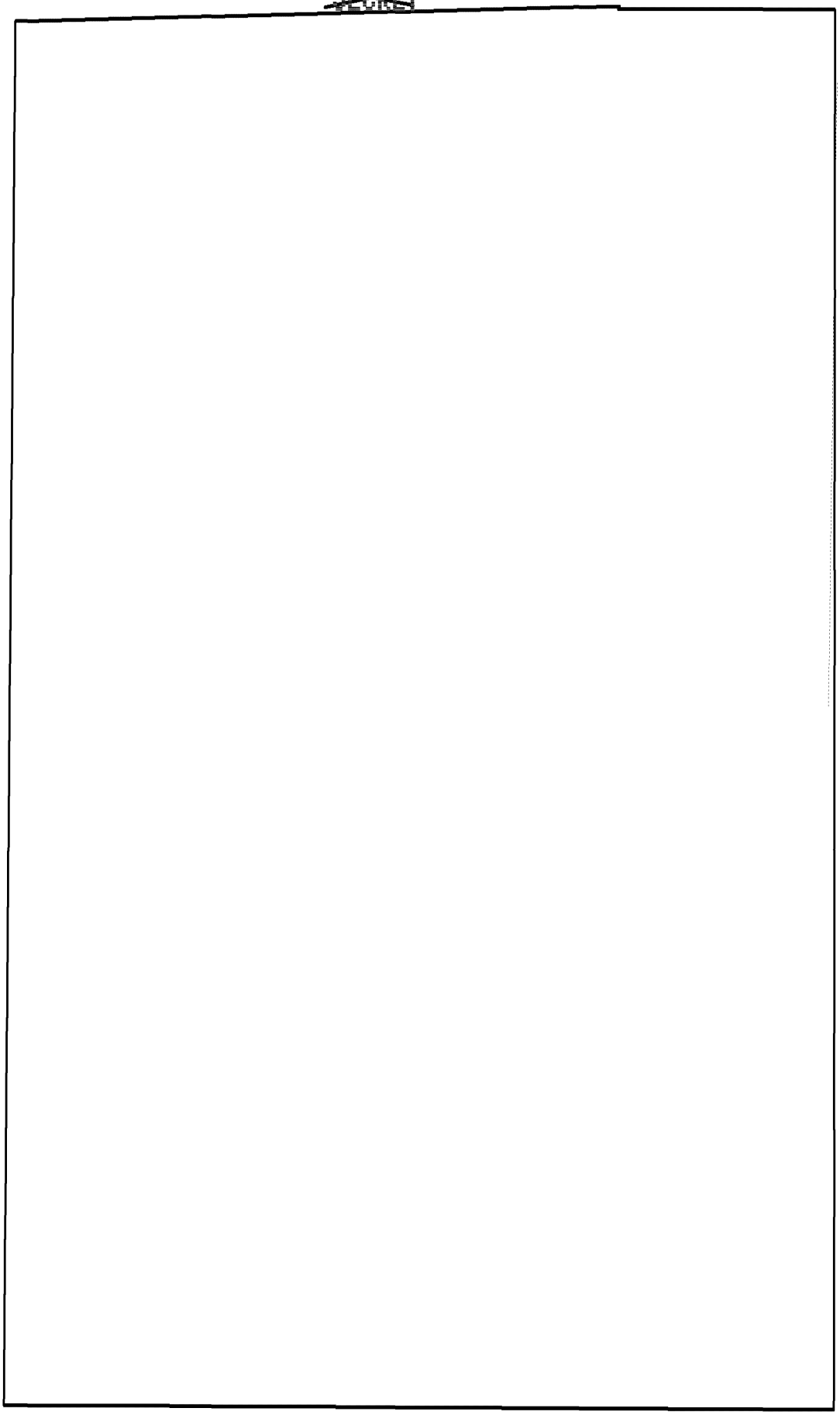


b1
b2
b7A
b7E

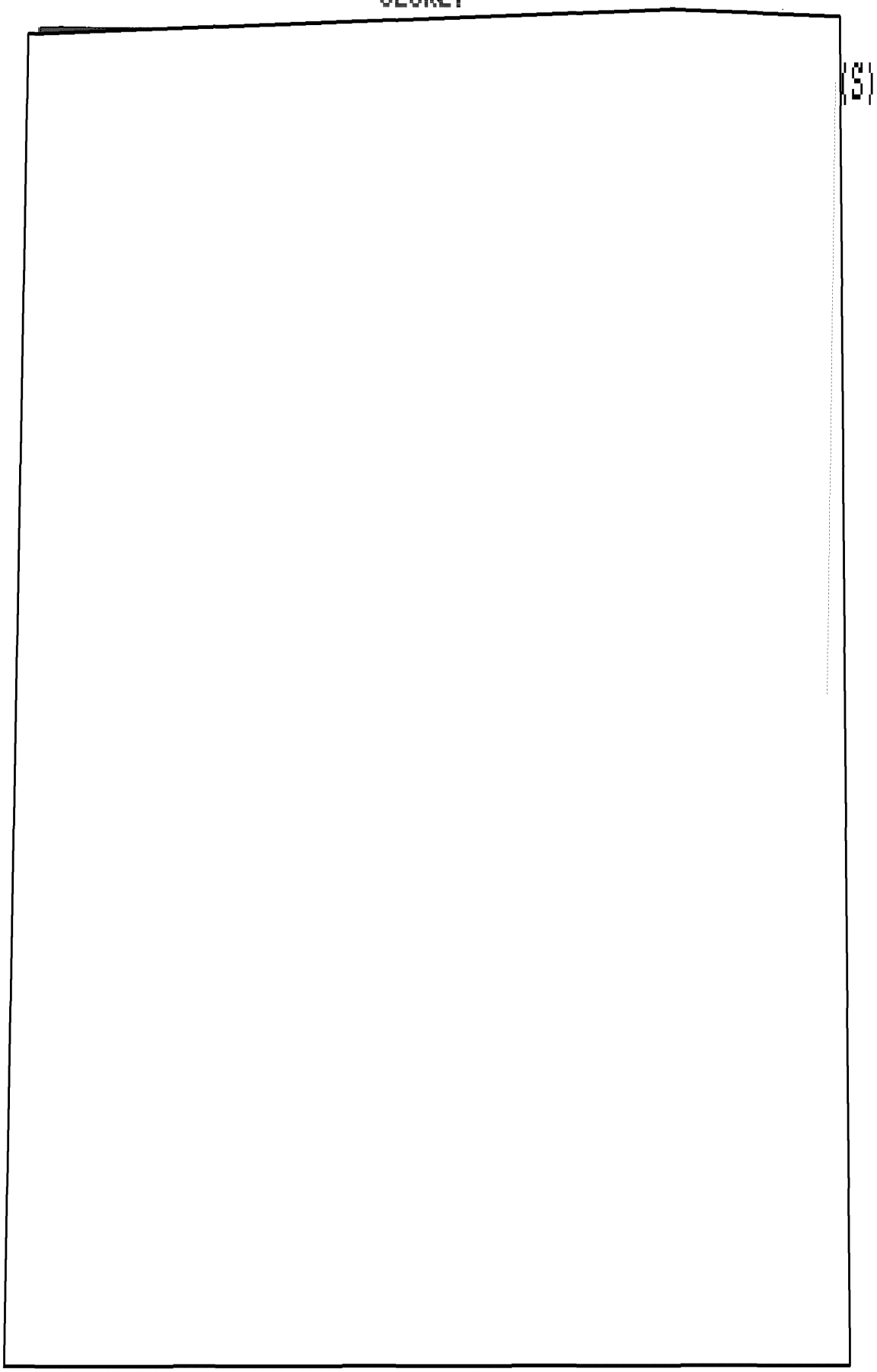


b1
b2
b7A
b7E

(S)



b1
b2
b7A
b7E



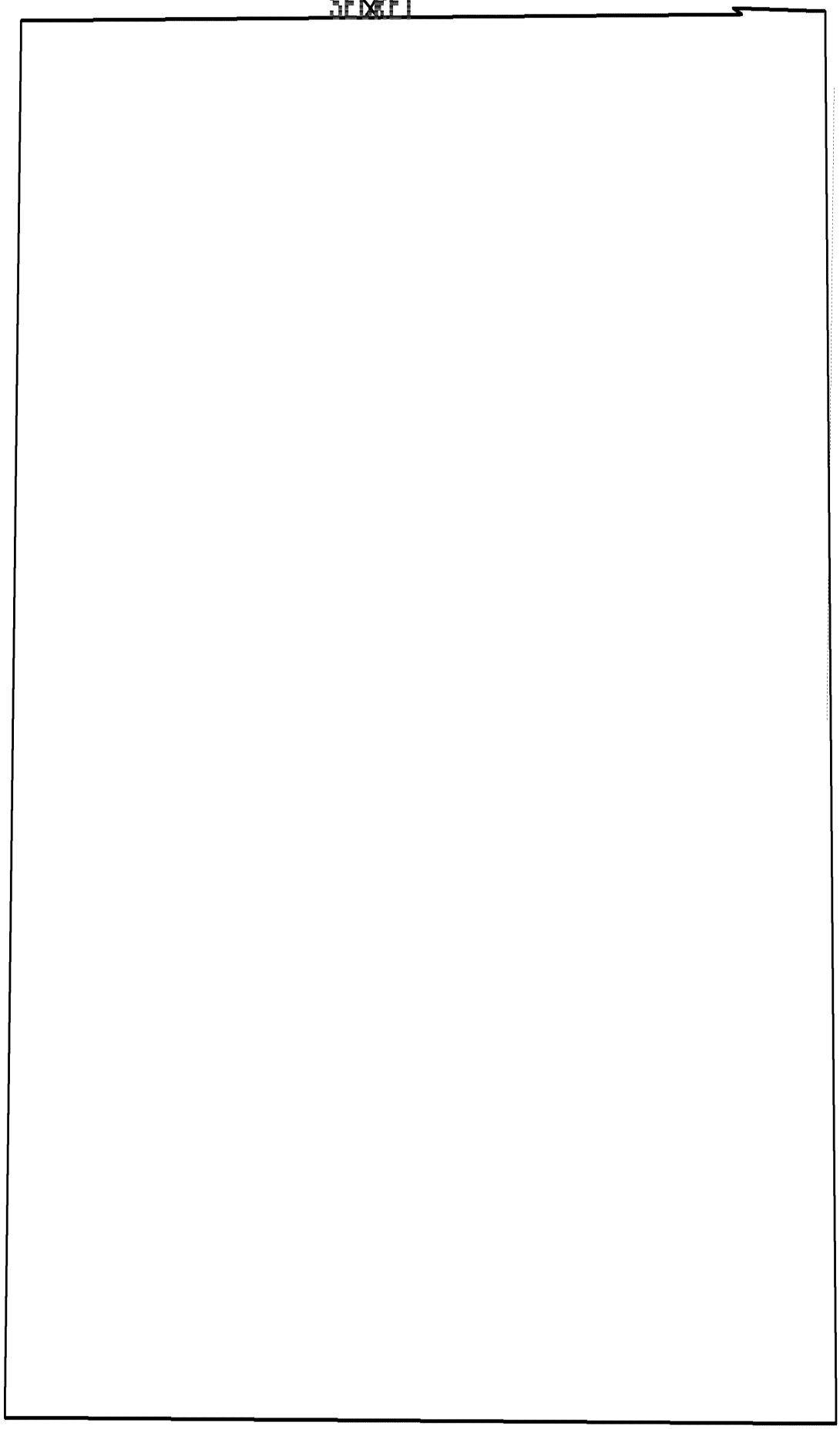
(S)

b1

b2

b7A

b7C



(S)

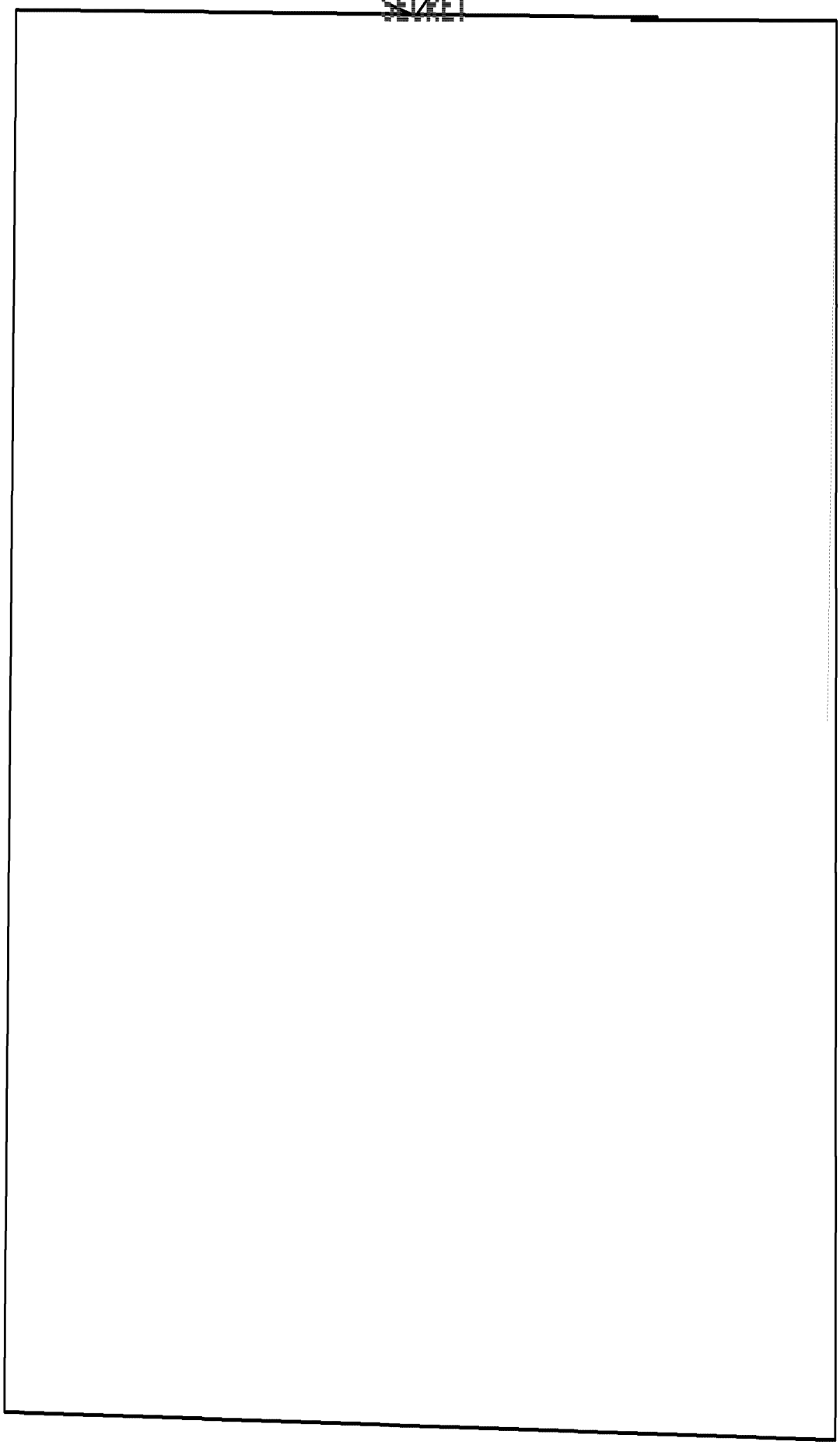
b1

b2

b7A

b7E

(S)



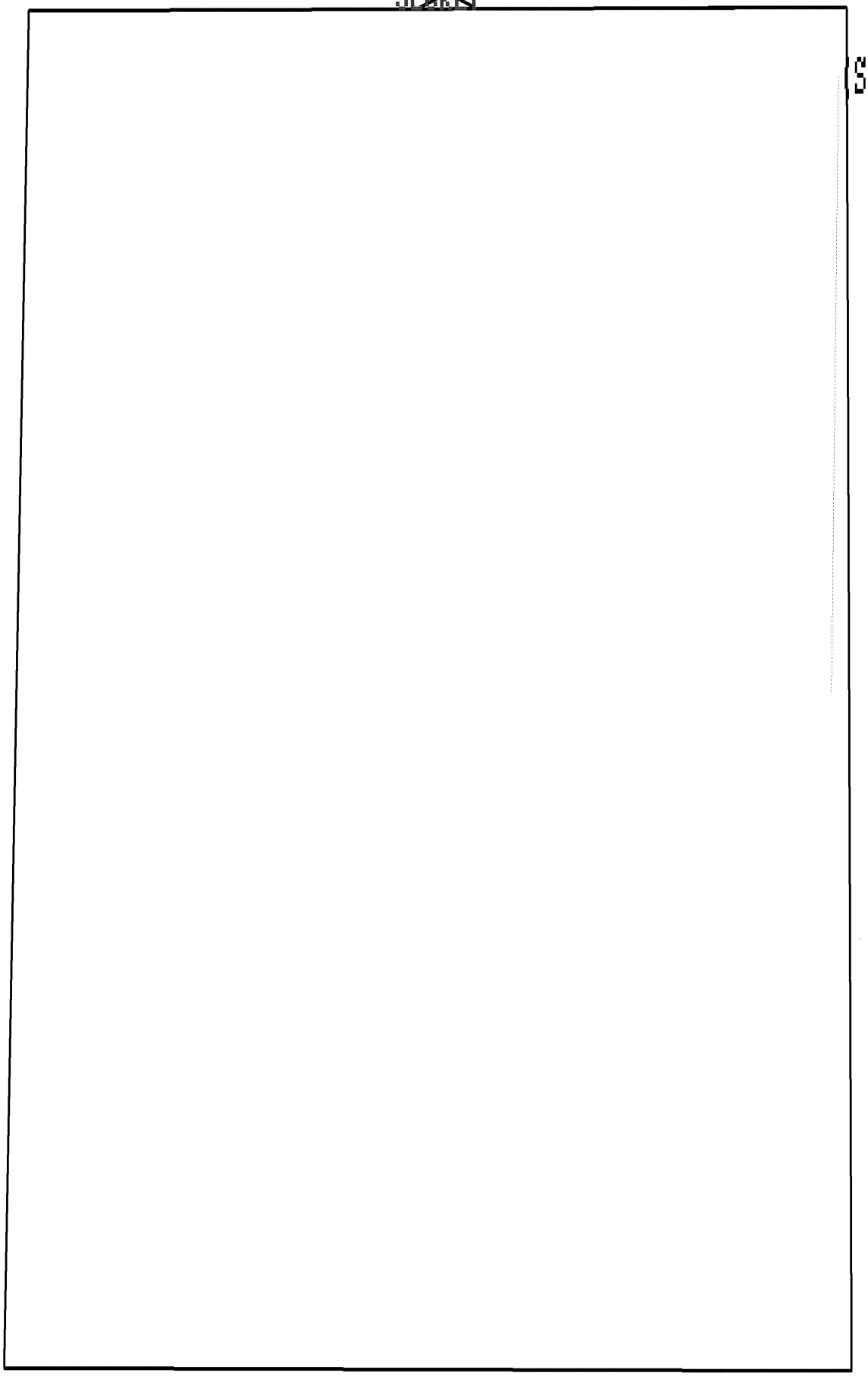
b1

b2

b7A

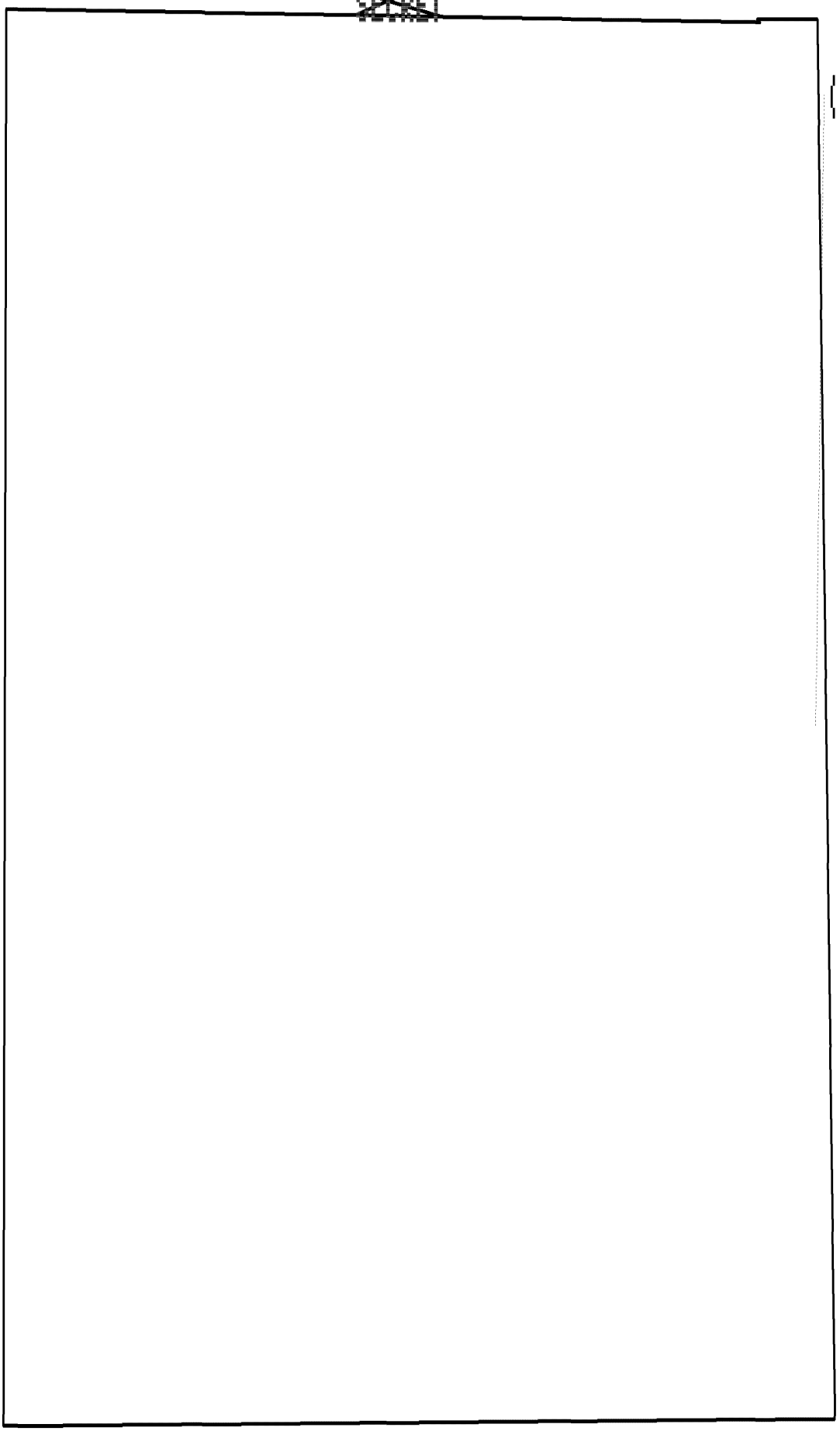
b7E

(S)



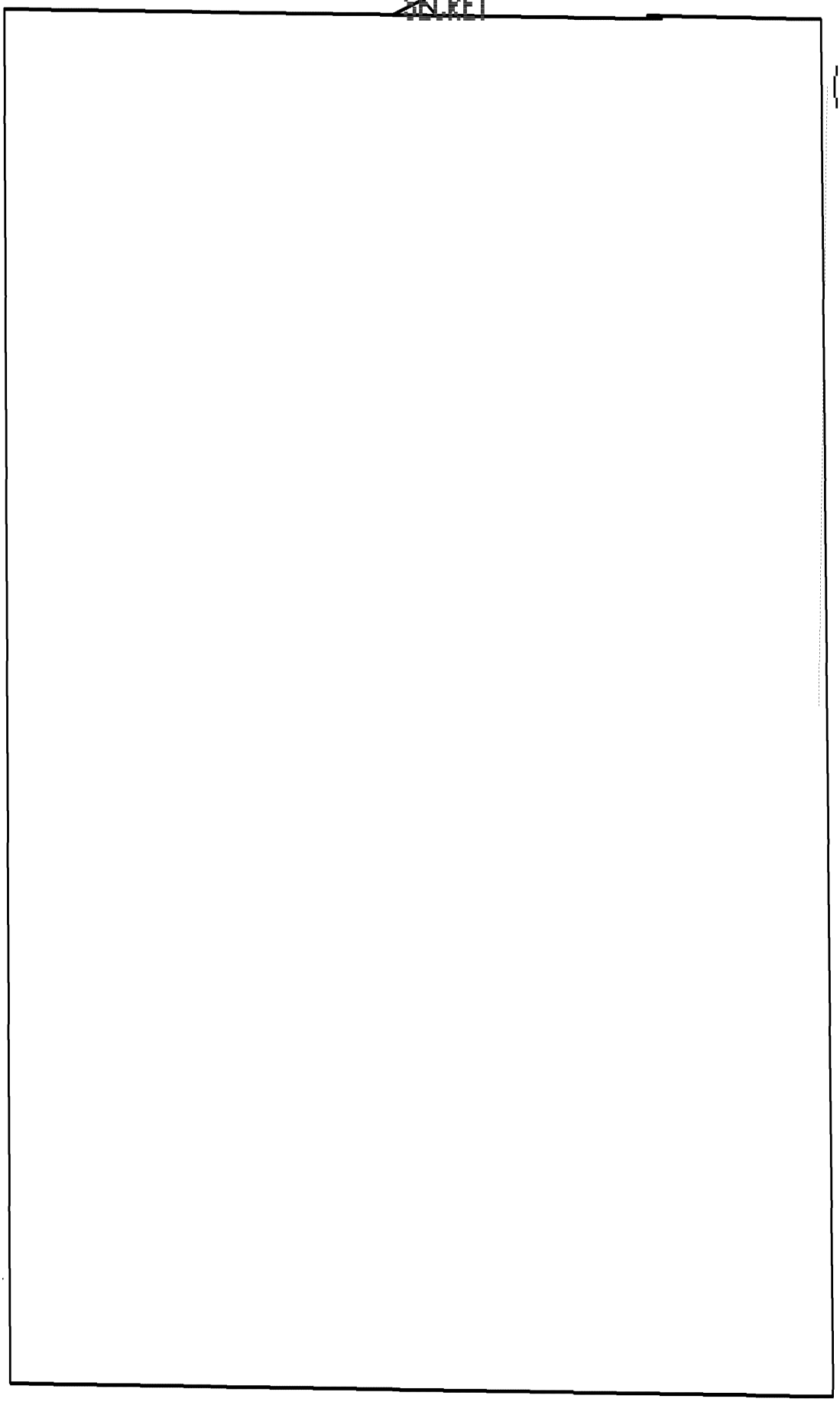
b1
b2
b6
b7A
b7C
b7E

(S)



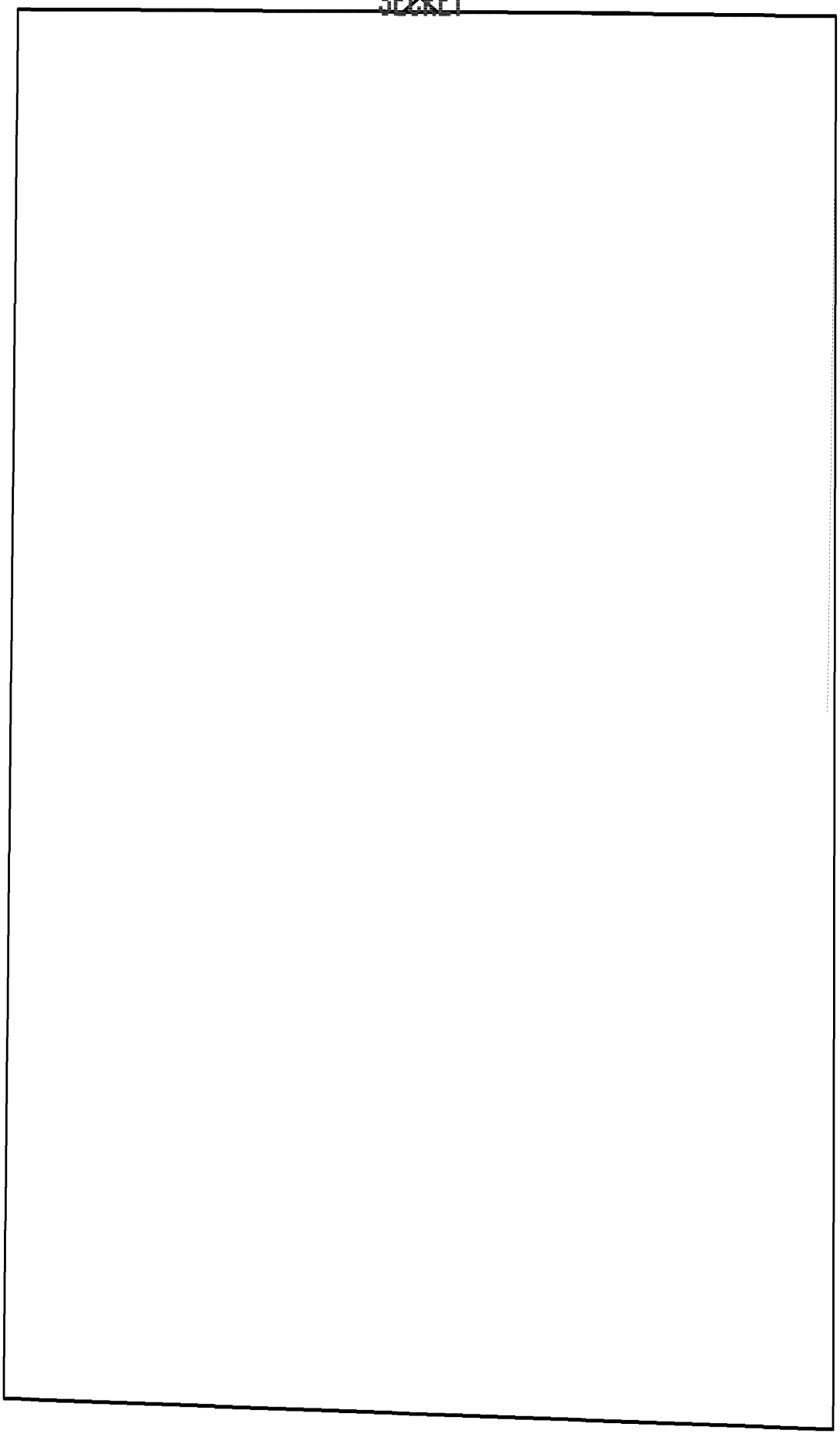
b1
b2
b6
b7A
b7C
b7E

(S)



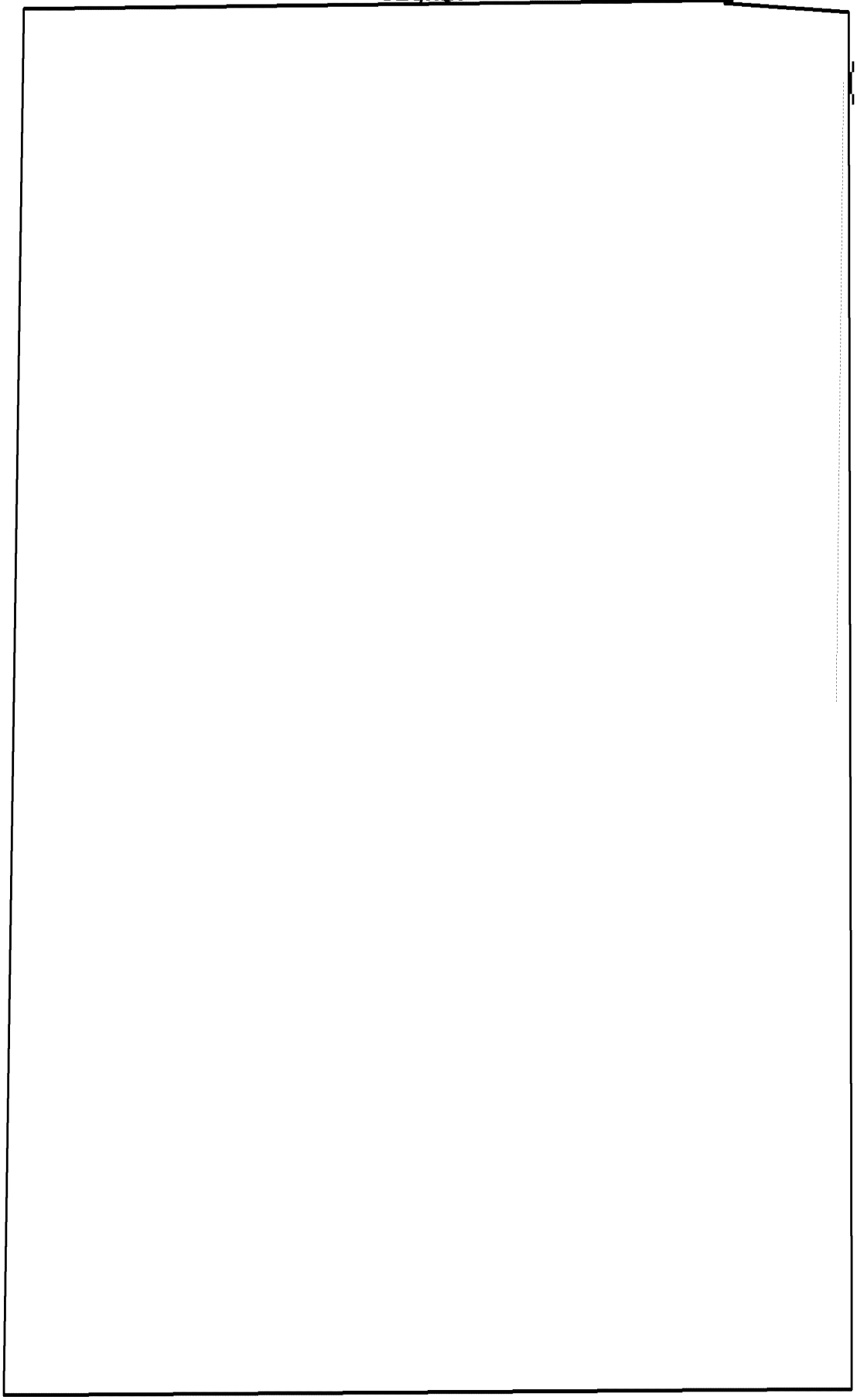
b1
b2
b6
b7A
b7C
b7E

(S)

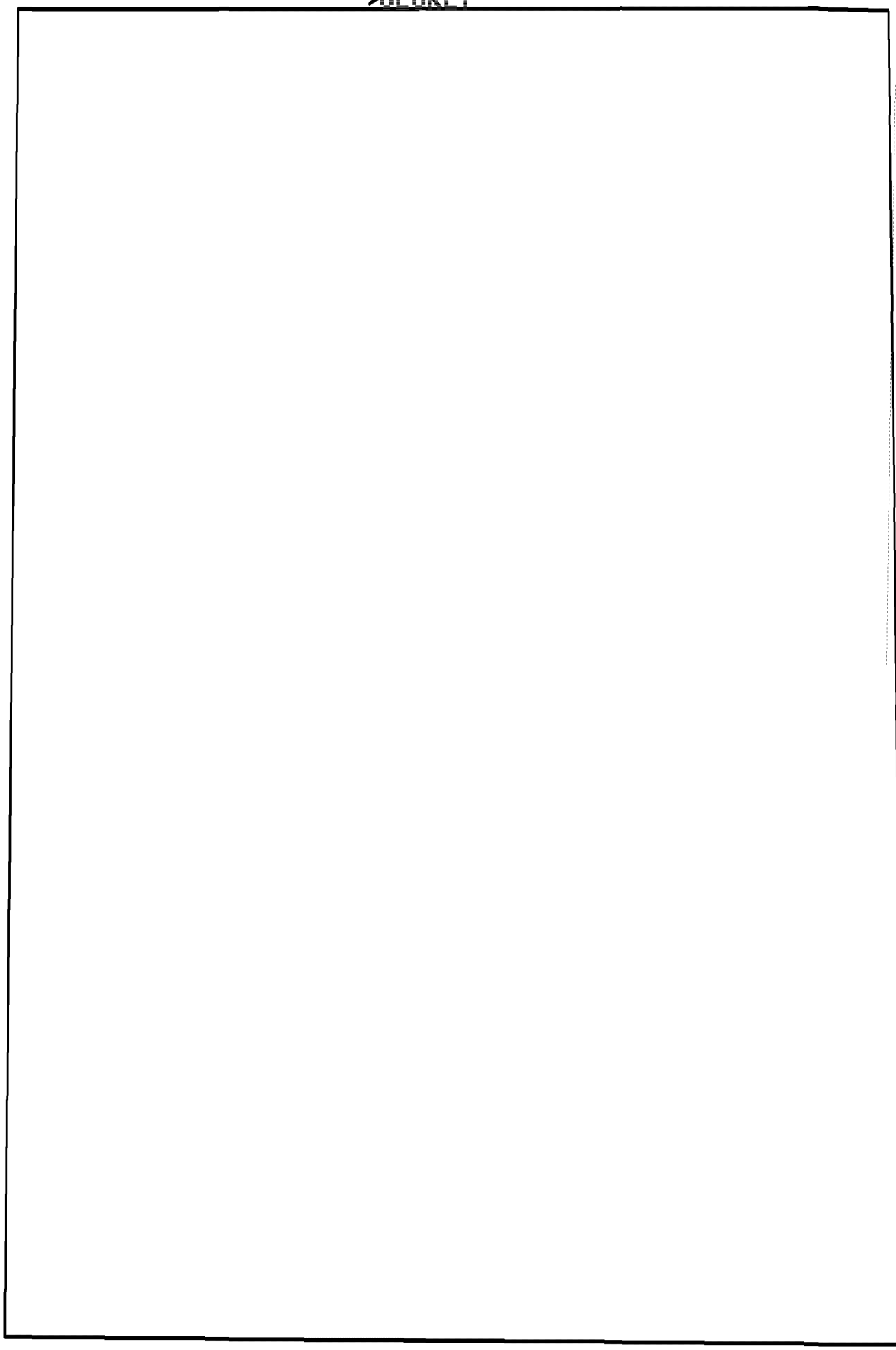


b1
b2
b6
b7A
b7C
b7E

(S)

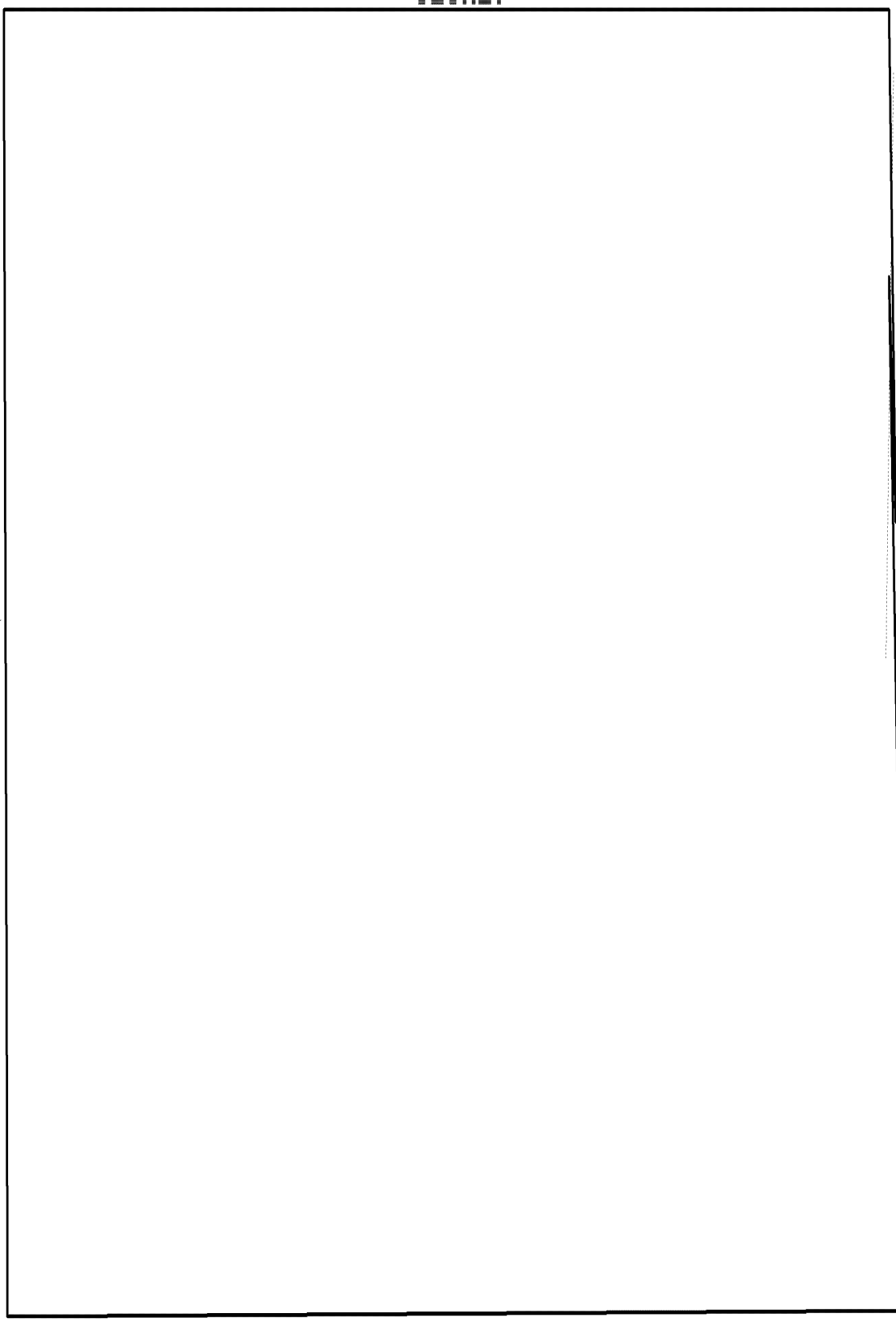


b1
b2
b6
b7A
b7C
b7E



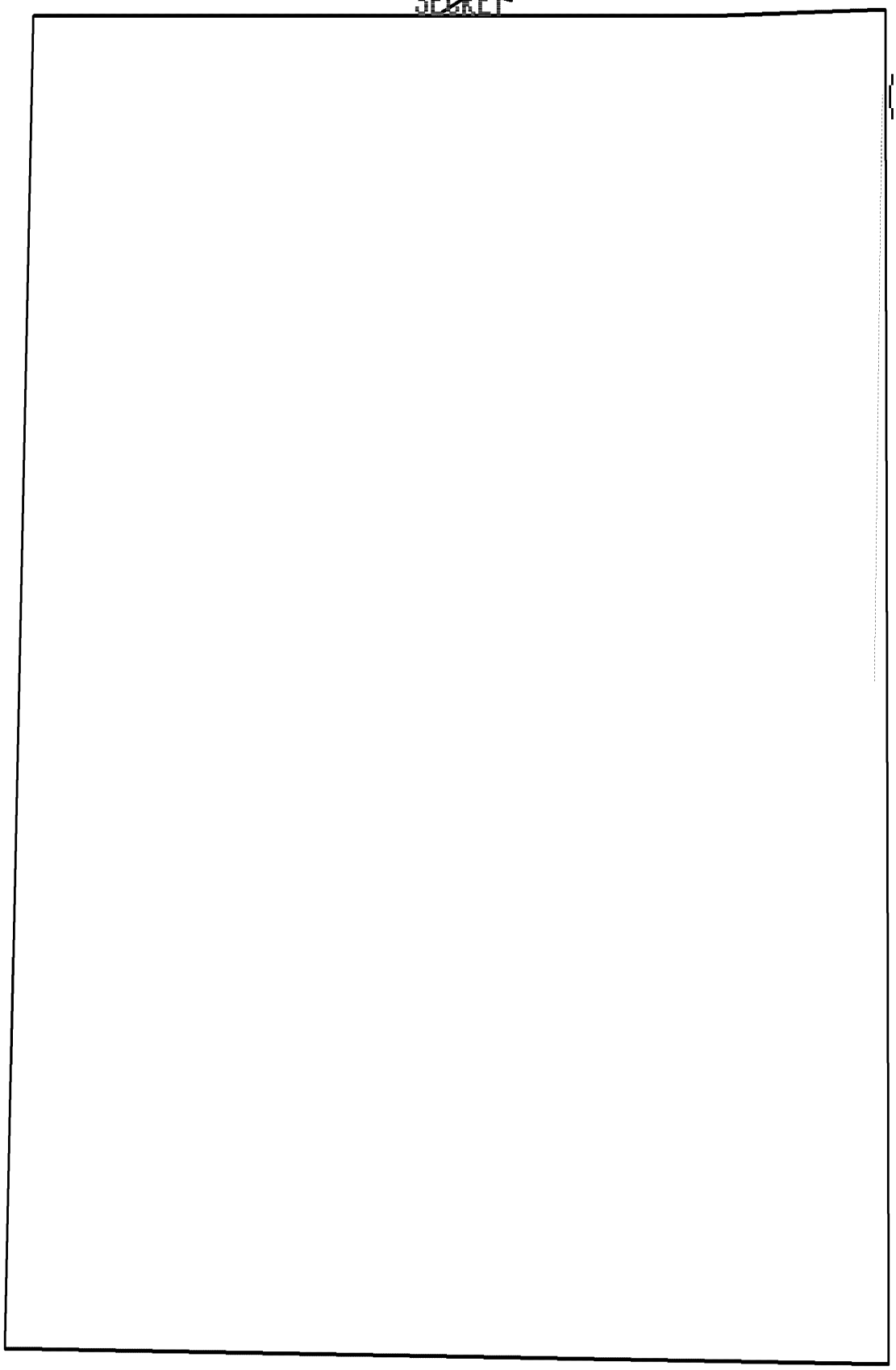
(S)

b1
b2
b6
b7A
b7C
b7E



(S)

b1
b2
b6
b7A
b7C
b7E



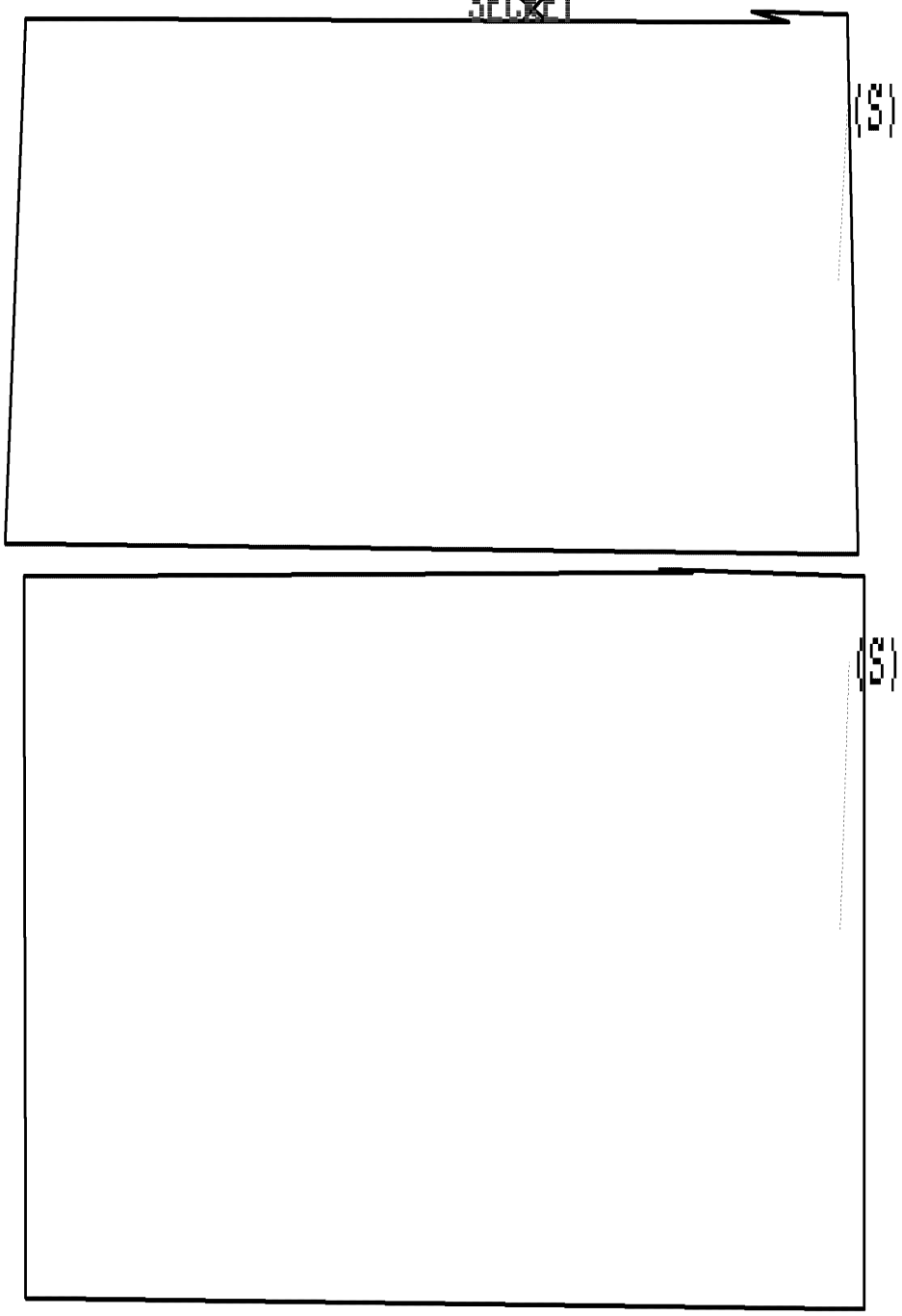
(S)

b1

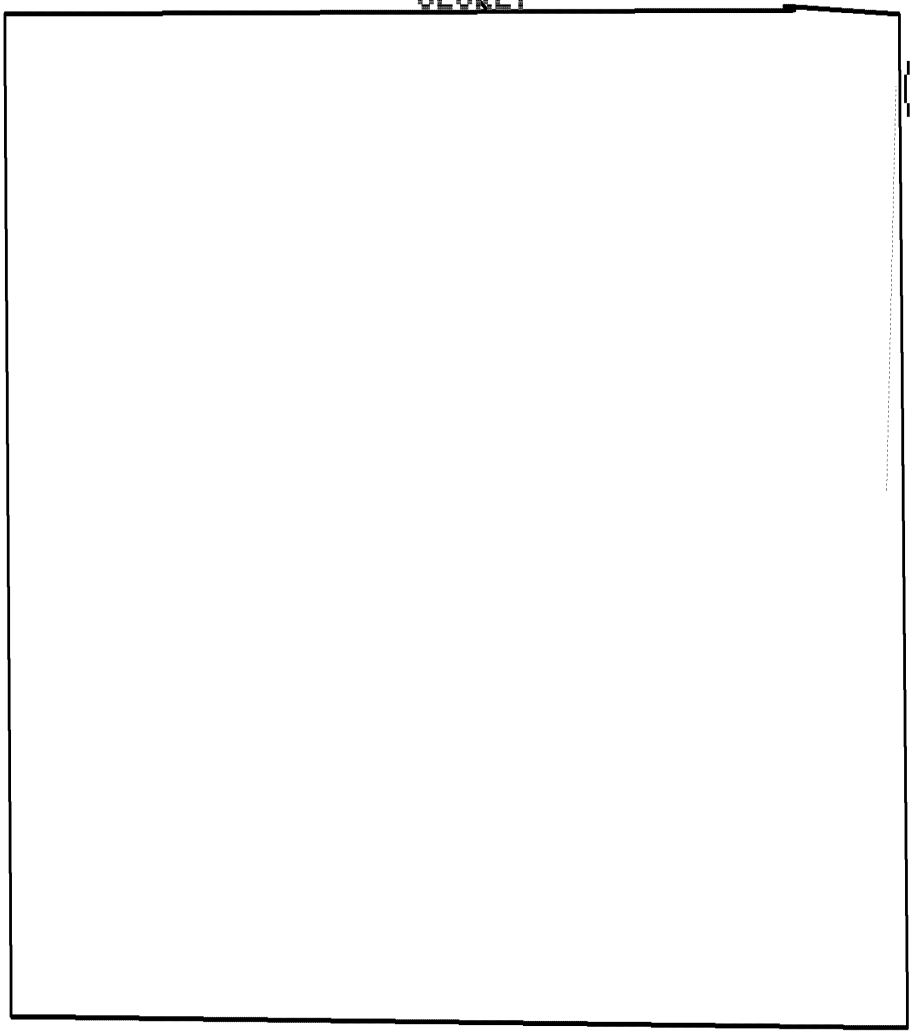
b2

b7A

b7E



b1
b2
b7E

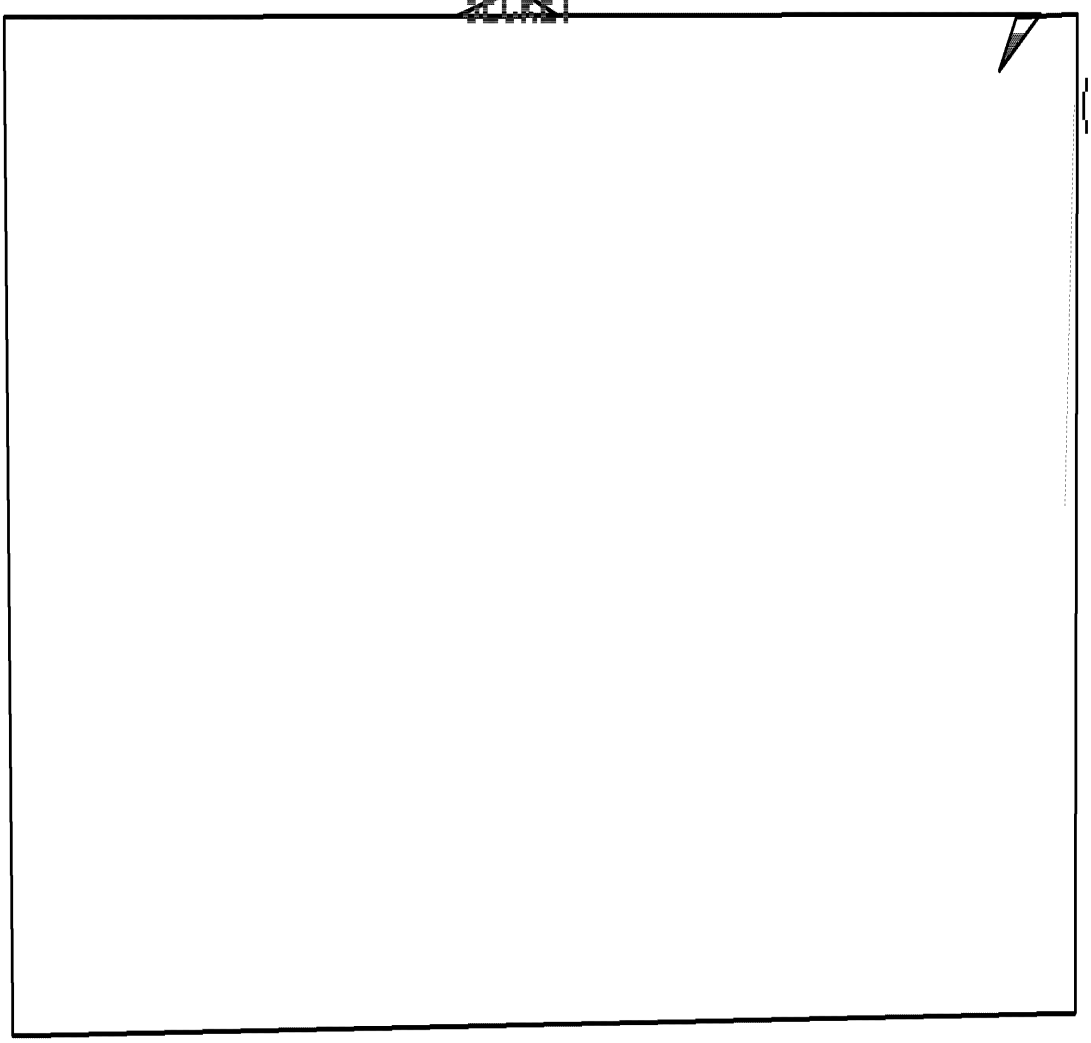


(S)

b1

b2

b7E



(S)

b1

b2

b7E

From: KALISCH, ELENI P. (OCA) (FBI) b6
Sent: Friday, March 25, 2005 11:26 AM b7C
To: [redacted] (OCA) (FBI) b2
Subject: FW [redacted] DIVISION PATRIOT ACT EXAMPLES b7E

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED # 05-CV-0845
DATE 08-23-2005 BY 65179 DMH /JHF

-----Original Message-----
From: [redacted] FBI)
Sent: Friday, March 25, 2005 11:24 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] FBI); [redacted] FBI); [redacted] (FBI)
Subject [redacted] DIVISION PATRIOT ACT EXAMPLES

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Eleni,

[redacted] Division references your email dated March 17, 2005, concerning the request for reporting Division Patriot Act examples. In 2002, [redacted] implemented a tracking report regarding use of various Patriot Act provisions, which are noted in the attached two statistical reports.

If you have any questions, you may contact Paralegal Specialis [redacted] at [redacted]

[redacted]

b2
b6
b7C
b7E

UNCLASSIFIED

UNCLASSIFIED

DATE: 09-19-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (c)
DECLASSIFY ON: 09-19-2030

From: [redacted] FBI) b2 b6 b7C b7E
Sent: Tuesday, March 29, 2005 7:47 AM
To [redacted] OCA) (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Subject: RE: Follow-up re [redacted] Examples - Patriot Act

~~UNCLASSIFIED~~
~~NON-RECORD~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]

Please review the below (blue) responses you requested from the [redacted] Division concerning the Patriot Act. If you need further info, you may reach me at [redacted] b2 b6 b7C b7E

[redacted]
Paralegal Specialist
[redacted]

-----Original Message-----
From: [redacted] (OCA) (FBI) b2 b6 b7C b7E
Sent: Friday, March 25, 2005 1:44 PM
To: [redacted] (FBI); [redacted] (FBI)
Subject: Follow-up re [redacted] Examples

UNCLASSIFIED
NON-RECORD

Thanks very much for your input re the Patriot Act. I have a couple of questions re the specific examples below, as follows:

b1 b2 b6 b7A b7C b7E

[redacted] (S)

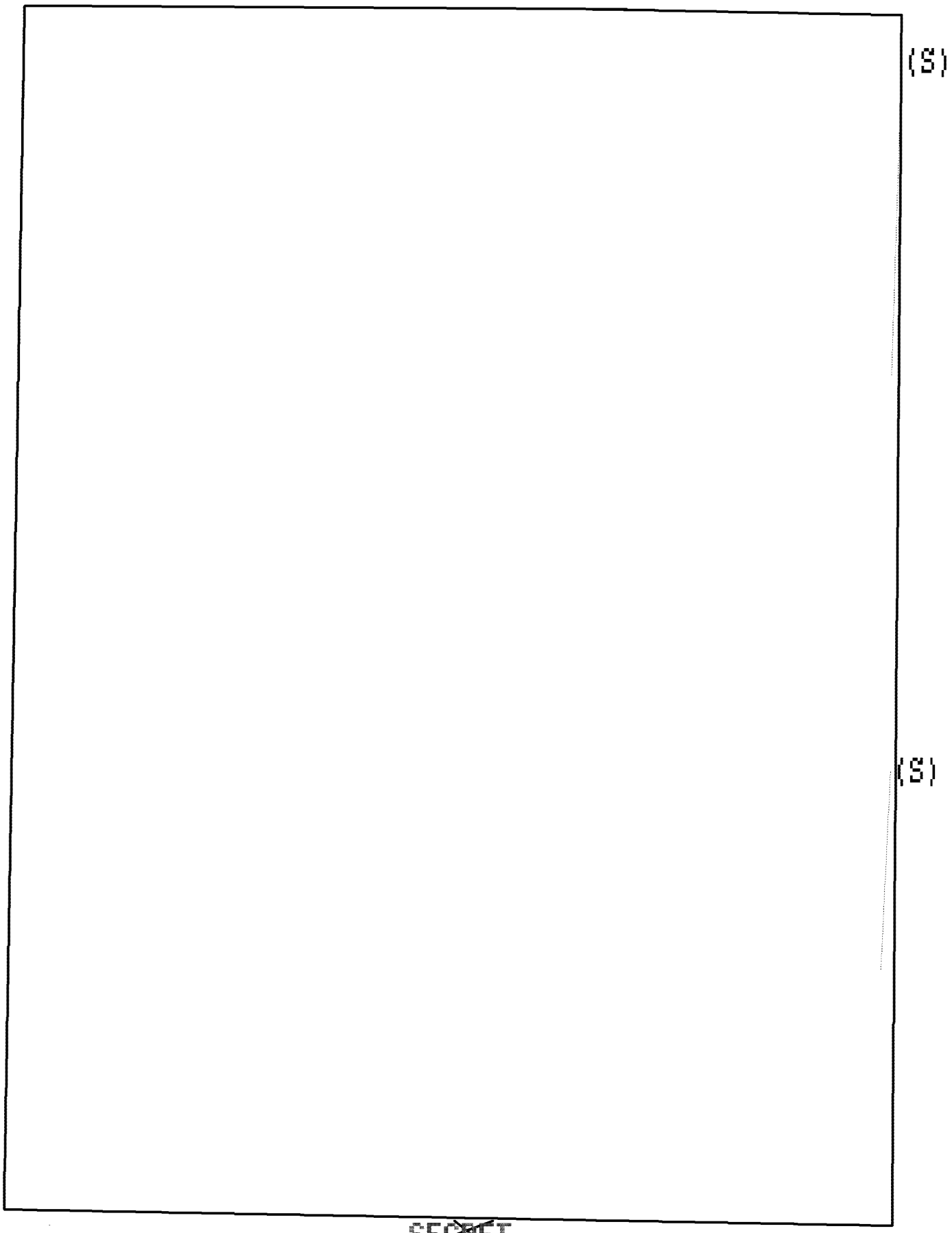
[redacted] (S)

~~SECRET~~

(S)

b1
b2
b7A
b7E

(S)



(S)

(S)

b1
b2
b6
b7C
b7E

(S)

b1
b2
b6
b7C
b7E

UNCLASSIFIED

UNCLASSIFIED

SECRET

(S)

b1
b2
b7E

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Wednesday, March 30, 2005 7:55 AM
To: [redacted] OCA) (FBI) b6 b7C
Subject: FW: Patriot Act Examples

~~UNCLASSIFIED~~
~~NON-RECORD~~

DATE: 09-19-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (c)
DECLASSIFY ON: 09-19-2030

-----Original Message-----
From: [redacted] FBI) b2 b6
Sent: Tuesday, March 29, 2005 5:44 PM
To: KALISCH, ELENI P. (OCA) (FBI) b7C
Cc: [redacted] (FBI) b7E
Subject: Patriot Act Examples

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

UNCLASSIFIED
NON-RECORD

Ms. Kalisch: b2

By e-mail of 3/17/05, you asked for unclassified examples wherein specific Patriot Act provisions were used. b7E The [redacted] Division was polled and the following are a summary of responses received.

With regard to the use of **Section 214**, which deals with FISA Pen Registers and Traps and Traces, that technique has been used in [redacted] cases with the following results:

[redacted] (S)

b1
b2
b7E

SECRET

My apologies for submitting this late.

b2
b6
b7C
b7E

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

SECRET

Message ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE PER OGA LET. DTD. 8/30/05

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 24, 2005 6:31 PM
To: [redacted] (OCA) (FBI) b6 b7C
Subject: FW: Declassification ~~SECRET~~

~~UNCLASSIFIED~~
~~NON-RECORD~~

DATE: 08-23-2005
CLASSIFIED BY 65179 DMH / JHF 05-CV-0845
REASON: 1.4 (c)
DECLASSIFY ON: 08-23-2030

FYI
-----Original Message-----
From: Caproni, Valerie E. (OGC) (FBI)
Sent: Thursday, March 24, 2005 6:24 PM
To: BALD, GARY M. (DO) (FBI); PISTOLE, JOHN S. (DO) (FBI); SZADY, DAVID (CD) (FBI); BAGINSKI, MAUREEN A. (DO) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] OGC)(FBI); BEREZNAY, TIMOTHY D. (CD) (FBI); HULON, WILLIE T. (CTD) (FBI); [redacted] (OI)(FBI) b6 b7C
Cc: KALISCH, ELENI P. (OCA) (FBI); CHANDLER, CASSANDRA M. (OPA) (FBI); STEELE, CHARLES M (DO)(FBI)
Subject: Declassification

~~UNCLASSIFIED~~
~~NON-RECORD~~

In connection with the run up to the Patriot Act hearings, the AG would like to publically disclose some data. Please let me know if you have a view, pro or con, and how strongly you feel about the issue. This is what they want to disclose:

1. 215: how many times the authority has been used, and the number of times it has been used to obtain specific categories of information.

So you know, the answer is: it has been used precious little -- I am guessing less than [redacted] times. The primary category of information that has been obtained is [redacted] (S) (S)

The one maybe dicey use was for [redacted] is confirming that order was eventually signed.] b1 b2 b6 b7C b7E

2. 215: how it hasn't been used. I don't know for sure, but I assume the AG would like to say we've never used it to get library or medical records.

3. FISA pen registers

a. The annual number of FISA pen registers.

b. A hypothetical explaining the benefits of pens. I don't have it yet, but more generally the question is: are FISA pens all that valuable? [redacted] but are they of much value to us?

4. The number of estimated person hours saved because of the longer renewal periods on FISAs. [OIPR is developing this number.]

The AGs office wants an answer by COB Friday, so please let me know ASAP.

~~SECRET~~

~~UNCLASSIFIED~~

UNCLASSIFIED

SECRET

From: [redacted] (FBI)
Sent: Monday, March 28, 2005 11:54 AM
To: [redacted] OCA) (FBI)
Subject: RE: PATRIOT ACT EXAMPLES

DATE: 12-29-2005
CLASSIFIED BY 65179DMH/BAW 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-29-2030

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I finally got a response, and was advised that #5 - jeopardizing an investigation, was the reason cited in both delayed notice warrants.
[redacted]

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Friday, March 25, 2005 11:23 AM
To: [redacted] FBI)
Subject: FW: PATRIOT ACT EXAMPLES

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] thanks very much for the examples below. Can you find out which of the [redacted] specific (S) circumstances was cited in the delayed notice warrants?

b1
b2
b7E

****

Pursuant to section 213, prosecutors can seek a judge's approval to delay notification by making a showing that if notification were made contemporaneous to the search, there is reasonable cause to believe one of the following might occur:

1. notification would reasonably endanger the life or physical safety of an individual;
2. notification would reasonably be expected to cause flight from prosecution;
3. notification would reasonably be expected to result in destruction of, or tampering with, evidence;
4. notification would reasonably result in intimidation of potential witnesses; or
5. notification would reasonably be expected to cause serious jeopardy to an investigation or unduly delay a trial.

****

Please call if you have questions. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 1:17 PM
To: [redacted] OCA) (FBI)
Subject: FW: PATRIOT ACT EXAMPLES

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----

SECRET

b2
b6
b7C
b7E

From: [redacted] (FBI)
Sent: Friday, March 25, 2005 1:11 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: FW: PATRIOT ACT EXAMPLES

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----

~~**SENSITIVE BUT UNCLASSIFIED**~~
~~**NON-RECORD**~~

b2
b6
b7C
b7E

Per your E-mail request of March 17, 2005, attached please find unclassified examples of how various Patriot Act provisions have benefitted the [redacted] Division. Should you need additional information, the [redacted] Office Point of Contact is SSA [redacted] telephone number [redacted]

Sections 203 & 218 - Information Sharing (S)

These sections provided new information sharing capabilities between criminal and intelligence investigations for foreign intelligence information and information obtained via a Title III electronic surveillance. The [redacted]D has disclosed foreign intelligence information obtained through the interception of wire, oral, and electronic communications [redacted] to other federal law enforcement, intelligence, protective, immigration, national defense or national security officials in order to assist the official receiving the information in the performance of his/her official duties. A partial list of the recipients of this foreign intelligence information includes [redacted] the Bureau of Immigration and Customs Enforcement, [redacted] and the Defense Intelligence Agency. The foreign intelligence information shared was related to the national security and defense of the United States as well as clandestine intelligence activities by agents of a foreign power.

b1
b2
b7E

Section 212 - Voluntary Disclosures

[redacted] (S)

b1
b2
b6
b7C
b7E

Section 213 - Delayed Notice of the Execution of a Warrant (Not a "sunset" provision, but examples were requested.)

(S) [redacted]

b1
b2
b7E

(S)

~~SECRET~~

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SECRET

From: KALISCH, ELENI P. (OCA) (FBI) b6
Sent: Friday, March 25, 2005 1:17 PM b7C
To: [redacted]OCA) (FBI)
Subject: FW: PATRIOT ACT EXAMPLES

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

DATE: 09-19-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-19-2030

-----Original Message-----
From [redacted](FBI) b2
Sent: Friday, March 25, 2005 1:11 PM b6
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: FW: PATRIOT ACT EXAMPLES b7C
b7E

~~**SENSITIVE BUT UNCLASSIFIED**~~
~~**NON-RECORD**~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message----- b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b7E

Per your E-mail request of March 17, 2005, attached please find unclassified examples of how various Patriot Act provisions have benefitted the [redacted] Division. Should you need additional information, the [redacted] Office Point of Contact is SSA [redacted] telephone numbe[redacted]

Sections 203 & 218 - Information Sharing (S)

These sections provided new information sharing capabilities between criminal and intelligence investigations for foreign intelligence information and information obtained via a Title III electronic surveillance. The [redacted]D has disclosed foreign intelligence information obtained through the interception of wire, oral, and electronic communications [redacted]to other federal law enforcement, intelligence, protective, immigration, national defense or national security officials in order to assist the official receiving the information in the performance of his/her official duties. A partial list of the recipients of this foreign intelligence information includes [redacted]the Bureau of Immigration and Customs Enforcement[redacted] and the Defense Intelligence Agency. The foreign intelligence information shared was related to the national security and defense of the United States as well as clandestine intelligence activities by agents of a foreign power.

b1
b2
b7E

Section 212 - Voluntary Disclosures

[redacted] (S)

b1
b2
b6
b7C
b7E

Section 213 - Delayed Notice of the Execution of a Warrant (Not a "sunset" provision, but examples were

(S) (S)

requested.)

The [ ]D has [ ] and searches of [ ] based on orders provided by the U.S. Foreign Intelligence Surveillance Court, in which the notice of the execution of the respective search warrant was delayed [ ] the foreign intelligence obtained as a result of the search has provided extensive leads for each investigation and has led to the identification of other agents of a foreign power involved [ ]

b1
b2
b7E

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SECRET

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Monday, March 28, 2005 7:37 AM
To: [redacted] (OCA) (FBI)
Subject: FW: Cyber Patriot Act Examples

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted] CyD) (FBI)
Sent: Friday, March 25, 2005 6:01 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: Cyber Patriot Act Examples

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Eleni,

Per your request, please see the attached from CyD.

Thanks, [redacted]

[redacted]
FBIHQ Cyber Division
Room 5853
[redacted]@ic.fbi.gov

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

b2
b6
b7C
b7E

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Monday, March 28, 2005 12:55 PM
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act Examples.. [redacted] Division

Importance: High

UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted] (FBI)
Sent: Monday, March 28, 2005 12:52 PM
To: KALISCH, ELENI P. (OCA) (FBI); [redacted] (OCA) (FBI)
Subject: Patriot Act Examples. [redacted] Division
Importance: High

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

AD Kalisch-

The attached is being provided as a result of your solicitation of examples re the PATRIOT Act.

Regards-

[redacted]
ASAC [redacted]

b2
b7E

[redacted] Division has reviewed provisions of the Patriot Act for any examples of how these provisions have been helpful to us in our investigative programs. This review has found an example of Section 203 (Information Sharing), which was beneficial as described here below:

b2
b7E

Title III Intelligence Information-Sharing by Criminal Investigators:

Section 203: Amends Title III, 18 USC Section 2517 to add subsection (6), to permit disclosure of Title III information when the matter involves foreign intelligence or counterintelligence information "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official...to assist the official who is to receive that information in the performance of his official duties."

In December 2004, ICE [redacted] provided FBI [redacted] with a Title III Application containing probable cause to believe that targeted subjects, and others yet unknown, have committed, are committing and will continue to commit offenses enumerated in Section 2516 of Title 18, USC, in violation of:

b2
b7E

(a) Title 18, USC, Section 2339 (A); providing material support to terrorists;

(b) Title 18, USC, Section 2339 (B); providing material support or resources to designated foreign terrorist organizations;

(c) Title 50, USC, Section 1701 et. al (Executive Order 13129 dated July 4, 1999 - International Emergency Economic Powers Act).

The above information was also disseminated to the appropriate CTD Units at FBIHQ. Once deconfliction was undertaken, it was determined by CTD that this information should initially be utilized [redacted] b2 b7E These coverages have been initiated by the [redacted] Division JTTF, which has assigned this investigative matter to an ICE SA, and is being jointly worked by FBI, ICE, and TFOs from other JTTF law enforcement entities.

UNCLASSIFIED

UNCLASSIFIED

The [redacted] Division has recently brought a pending international terrorism investigation to a new level with the arrest of the main subject and two associates. The arrests were based on indictments which had until recently, been sealed. The indictment charges the subjects with violations including Immigration Fraud, Distribution of Drug Paraphernalia, Money Laundering, Bank Fraud and Conspiracy. A charge of Providing Material Support to a Terrorist Organization is being held in abeyance at this time [redacted]

b2
b7E

[redacted]

b1

This investigation commenced two years ago based on information that the subject had arrived in the United States on a fraudulent immigrant visa and that the subject associated with the subjects of pending terrorism investigations in the [redacted] Division. Shortly after [redacted] initiated this investigation, information was provided to the FBI liaison to the JTTF

b2
b7E

(S)

(S)

The main subject and two associates were recently arrested. With the threat of a long incarceration, seizure of assets followed by subsequent deportation, [redacted]

b2
b7E

b1
b2
b7E

video-recorded and assigned to the JTTF. (S)

b1
b2
b7E

During the course of this investigation, all logical and necessary tools authorized under the USA PATRIOT Act were utilized to bring this investigation to a very favorable point at this time. were utilized as were Federal Grand Jury subpoenas, FGJ testimony and subsequent indictment and arrest which proved successful in causing the subject to provide (S)

POC for more information: SSA

b6
b7C

b2
b6
b7C
b7E

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 2:30 PM
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples - [redacted]Division

b7E ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179 DMH / JHF 05-CV-0845

Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted](FBI)
Sent: Friday, March 25, 2005 2:14 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI)
Subject: Patriot Act Examples - [redacted]Division
Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b6
b7C
b7E

Eleni,

As [redacted] I am the POC for all USA Patriot Act-related matters for [redacted] Please find below a synopsis of instances in which the [redacted] Division has utilized Patriot Act provisions, per your email request of March 18, 2005:

Section 206 (Roving Wiretaps) - [redacted]

b2
b7E

Section 213 (Delayed Notice Search Warrants) - [redacted]

b2
b7A
b7E

[redacted] NOTE: THIS CASE IS STILL CONTINUING IN A GROUP I UNDERCOVER STATUS AND CANNOT BE PUBLICLY REVEALED PRIOR TO INDICTMENT.

Section 217 (Computer Hacking victims requesting law enforcement assistance) - [redacted]

b2
b7A
b7E

This provision allowed access to much more information from the victim than would have likely been received prior to its implementation without a search warrant.

Section 220 (Nationwide Search Warrants for Electronic Evidence) - [redacted] has issued dozens of out-of-district ISP search warrants since October 2001. [redacted]

b2
b7A
b7E

[redacted] NOTE: THIS CASE IS STILL CONTINUING AND CANNOT BE PUBLICLY REVEALED PRIOR TO INDICTMENT.

Other warrants have been utilized to obtain information regarding Innocent Images/Child Pornography matters, as well as evidence of cyber intrusions.

b6
b7C

Obviously the fact that these examples have to be written up in an UNCLAS format has hindered our ability to detail exactly what the PATRIOT act provisions have enabled us to do since October 2001. Although you're probably already aware of this fact, some of these examples were previously provided to OGC attorney [redacted] Investigative Law Unit, who should have a plethora of illustrations you can use.

Please let me know if [redacted] can assist in any other way.

[redacted]

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

From: [redacted] (FBI) b2 b6 b7C b7E
Sent: Monday, March 28, 2005 11:49 AM
To: [redacted] (OCA) (FBI)
Cc: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI)
Subject: RE: Patriot Act Examples - [redacted] Division

Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

Circumstances 1, 3, 4 and 5 were cited in the affidavit as constituting a reasonable basis for the delay. I have included the pertinent paragraph from the affidavit for your reference.

Please let me know if you need any further information.

[redacted] b2 b6 b7C b7E

Reasonable Cause For Delay In Notification

57. As noted above, reasonable cause for delay in notification of the execution of a search warrant is established if it is shown that notification at the execution of the warrant may have an adverse result, to include endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation . The reasons in the instant case include, but are not limited to the following. Notice of the search at the time of the execution of the warrant is likely to place the cooperating witnesses and undercover agents in substantial danger. For example, [redacted] after cooperating in an earlier investigation, reported that [redacted] Persons involved in criminal activity in [redacted] have historically intimidated witnesses to prevent their cooperation with federal law enforcement agencies, to include threats of destruction of property and physical harm. Notice will allow the subjects of the investigation the opportunity to tamper with and destroy evidence, to include evidence of the payments made to local law enforcement officials and the disposition of proceeds of the illegal activities. Further, notice of the execution of the warrant at the time of its execution is likely to foreclose the future use of UCAs in the investigation, seriously jeopardizing the investigation. b2 b6 b7C b7D b7E

-----Original Message-----
From: [redacted] (OCA) (FBI) b2 b6 b7C b7E
Sent: Friday, March 25, 2005 2:35 PM
To: [redacted] (FBI)
Subject: FW: Patriot Act Examples - [redacted] Division
Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S) b1 b5 b6 b7C

[redacted] - in the delayed notice case, [redacted] (We won't describe your case, but we're trying to tally how many times we're citing to the specific circumstances). Thanks,

****

Pursuant to section 213, prosecutors can seek a judge's approval to delay notification by making a

showing that if notification were made contemporaneous to the search, there is reasonable cause to believe one of the following might occur:

1. notification would reasonably endanger the life or physical safety of an individual;
2. notification would reasonably be expected to cause flight from prosecution;
3. notification would reasonably be expected to result in destruction of, or tampering with, evidence;
4. notification would reasonably result in intimidation of potential witnesses; or
5. notification would reasonably be expected to cause serious jeopardy to an investigation or unduly delay a trial.

****

[redacted]
Office of Congressional Affairs
[redacted] b2

-----Original Message----- b6
From: KALISCH, ELENI P. (OCA) (FBI) b7C
Sent: Friday, March 25, 2005 2:30 PM b7E
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples - [redacted] Division
Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
-----Original Message----- b6
From: [redacted](FBI) b7C
Sent: Friday, March 25, 2005 2:14 PM b7E
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI)
Subject: Patriot Act Examples [redacted] Division
Importance: High

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b2
b6
Eleni, b7C

As [redacted] I am the POC for all USA Patriot Act-related matters for [redacted] Please find below a synopsis of instances in which the [redacted] Division has utilized Patriot Act provisions, per your email request of March 18, 2005: b7E

Section 206 (Roving Wiretaps) - In January - May 2004, FBI [redacted] repeatedly utilized this provision to [redacted] b2 b7E

Section 213 (Delayed Notice Search Warrants) - [redacted] b2 b7A b7E

[redacted] NOTE: THIS CASE IS STILL CONTINUING IN A GROUP I UNDERCOVER STATUS AND CANNOT BE PUBLICLY REVEALED PRIOR TO INDICTMENT.

Section 217 (Computer Hacking victims requesting law enforcement assistance) - [redacted] This provision allowed access to much more information from the victim than would have likely been received prior to its implementation without a search warrant.

Section 220 (Nationwide Search Warrants for Electronic Evidence) - [redacted] has issued dozens of out-of-district ISP search warrants since October 2001. [redacted] NOTE: THIS CASE IS STILL CONTINUING AND CANNOT BE PUBLICLY REVEALED PRIOR TO INDICTMENT.

Other warrants have been utilized to obtain information regarding Innocent Images/Child Pornography matters, as well as evidence of cyber intrusions.

Obviously the fact that these examples have to be written up in an UNCLAS format has hindered our ability to detail exactly what the PATRIOT act provisions have enabled us to do since October 2001. Although you're probably already aware of this fact, some of these examples were previously provided to OGC attorney [redacted] Investigative Law Unit, who should have a plethora of illustrations you can use.

Please let me know if [redacted] can assist in any other way.

[redacted]

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED

SECRET

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

b2
b6
b7C
b7E

From: [redacted] (FBI)
Sent: Monday, March 21, 2005 5:22 PM
To: [redacted] (OCA) (FBI)
Subject: RE: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

They are all unclassified - although sensitive. I am going to run the complete list past everyone here one more time and if there are any changes, then I will send them to you tomorrow.

-----Original Message-----
From: [redacted] OCA) (FBI)
Sent: Monday, March 21, 2005 1:36 PM
To: [redacted] (FBI)
Subject: RE: Patriot Act Examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

b2
b6
b7C
b7E

[redacted] - this is great. Before you head out, what is [redacted] position re the classification of the information contained in the write-up you provided?

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Monday, March 21, 2005 4:13 PM
To: [redacted] (FBI)
Cc: [redacted] OCA) (FBI)
Subject: FW: Patriot Act Examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

[redacted]
This is very helpful. If we need additional information, OCA [redacted] will contact you.
Thanks,
Eleni

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Monday, March 21, 2005 3:57 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: RE: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

Eleni,

b2

b7E

I am going to be the POC on this for the [redacted] Division. Attached is a draft that I have compiled from our agents. Would you mind taking a look at it and letting me know if you need more details or anything else. Otherwise, I will forward a very similar final draft to you tomorrow. I will be out of the office from 3/23 through 3/30.

Thanks.

[redacted]

[redacted] Division

[redacted]

b2

b6

b7C

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 9:07 AM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted]

b2

[redacted]

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Monday, March 21, 2005 4:13 PM
To: [redacted](FBI)
Cc: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

[redacted]
This is very helpful. If we need additional information, OCA [redacted] will contact you. b2
Thanks, b6
Eleni b7C
b7E

-----Original Message-----
From: [redacted](FBI)
Sent: Monday, March 21, 2005 3:57 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: RE: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

Eleni, b2
I am going to be the POC on this for the [redacted] Division. Attached is a draft that I have compiled from b7E
our agents. Would you mind taking a look at it and letting me know if you need more details or anything else. Otherwise, I will forward a very similar final draft to you tomorrow. I will be out of the office from 3/23 through 3/30.
Thanks.

[redacted] b2
b6
b7C
b7E

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 9:07 AM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

b1
b2
b6
b7A
b7C
b7E

Roving FISA surveillance (§§ 206):

(S)

Voluntary disclosure by ISP in emergencies (§§ 212):

(S)

b1
b2
b6
b7A
b7C
b7E

(S)

Section 214 - FISA Pen/Trap Authority

(S)

b1
b2
b6
(S) b7A
b7C
b7E

Monitoring communications of computer trespassers with victim consent (§§ 217):

(S)

b1
b2
b6
b7C
b7E

Nationwide search warrants for email (§§ 220):

[redacted] (S)

b1
b2
b6
b7C
b7E

Immunity from civil liability for those persons giving the FBI information in compliance with a FISA order (§§ 225):

[redacted] (S)

b1
b2
b6
b7A
b7C
b7E

From: KALISCH, ELENI P. (OCA) (FBI) b6
Sent: Wednesday, March 23, 2005 1:00 PM b7C
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples

DATE: 09-20-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-20-2030

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted](FBI) b2
Sent: Wednesday, March 23, 2005 12:56 PM b6
To: KALISCH, ELENI P. (OCA) (FBI) b7C
Cc: [redacted](FBI); [redacted](FBI); [redacted](FBI) b7E
Subject: Patriot Act Examples

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S) b2
Eleni, b7E

In response to your e-mail disseminated to the filed, dated 03/17/2005, concerning feedback on the utility of the Patriot Act sunset provisions, [redacted] after canvassing all relevant squads, responds as follows: b1

Since the inception of the Patriot Act, the [redacted] JTTF [redacted] JTTF) has [redacted] instances of use of the Expanded Title III Predicates (sections 201 and 202), Roving Wiretaps (section 206) or Computer Hacking Victims Requesting Law Enforcement Assistance (section 217). All pen registers currently and in the past three years that are being utilized by the [redacted] JTTF are being done via criminal justification. b2 b7A b7E

[redacted] (S)

The most common use of the Patriot Act on the [redacted] JTTF is for disseminating information in ACS that is terrorism related to state and local law enforcement (sections 203 and 218). To date, the [redacted] JTTF has provided information to [redacted] on [redacted] occasions. The [redacted] JTTF also coordinates information sharing with BICE, the Department of Homeland Security, the US Marshals, DEA, IRS, FAM, Air Force OSI, the US Secret Service, the [redacted] Attorney Generals Office, and [redacted] Police Departments under the same Patriot Act sections (203 and 218). b1 b2 b7C b7E

The [redacted] Division has been conducting a significant Bribery, Graft and Conflicts of Interest Title 18 U.S.C. Section 201 investigation involving large amounts of money laundering. [redacted] maintained corrupt relationships with [redacted] public officials designed to protect and enhance [redacted] financial interests. Due to the high profile nature of this case and the impact on [redacted] the [redacted] Division requested a USA Patriot Act Section 314 (a) disclosure of all banks with accounts, safe deposit boxes, and other 314(a) regarding our subjects in the case. In consultation with the Division's CDC and the United States Attorney's Office, it was decided that utilization of the Patriot Act provisions relating to money laundering would benefit the investigation. Although some publicity resulted from the requests made of the financial institutions, the resulting information was significant to the investigation. The overall outcome was positive and resulted in similar requests by other divisions to utilize the Patriot Act [redacted] b2 b6 b7C b7E

We hope this feedback, when coupled with input from other field offices, will aid in our preservation of the essential sunset provisions of the Patriot Act.

SSA [redacted] b6 b7C

SECRET

b2
b6
b7C
b7E

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

SECRET

From: [redacted] (FBI) b2 b6 b7C b7E
Sent: Tuesday, March 29, 2005 12:11 PM
To: [redacted] (OCA) (FBI)
Cc: [redacted] (FBI)
Subject: Use of the Patriot Act

SECRET
RECORD [redacted] b2 b7A b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE [redacted] b6 , b7C

DATE: 08-25-2005
CLASSIFIED BY 65179 DMH / JHF 05-CV-0845
REASON: 1.4 (C , D)
DECLASSIFY ON: 08-25-2030

Summerized below are several [redacted] Division cases where the use of the Patriot was an advantage for our investigations: b2 b7E

(S)

[redacted] b1 b2 b6 b7A b7C b7E

SECRET

(S)

b1
b2
b7A
b7E

During our weekly JTTF meetings we brief all cleared members with the most current intelligence which might affect our area as well as intelligence on terrorist plans and activities.

If you need any other information, please give me a call at [redacted] Thanks ASAC [redacted] b2 b7E

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
SECRET

Thanks,
ASAC [redacted] b2 b7E

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFY ON: 20150329~~
SECRET

SECRET

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

EXAMPLES OF PATRIOT ACT USED BY FBI [redacted]

b2
b7E

Section 212 - EMERGENCY DISCLOSURE OF EMAIL AND RECORDS BY ISPs

174A-[redacted]-66039

FBI [redacted] Comm Center received a bomb threat at 3:00 a.m. on 8/5/2004. After clarifying that the bomb threat was to the local airport and that the FBI had until noon to meet the caller's demands, FBI [redacted] JTTF Agents began tracing the caller id of the bomb threat. Investigation showed [redacted] The [redacted] provided investigators with [redacted] along with the date and time of registration of the individual who was responsible for making the bomb threat. **To obtain the subscriber information to actually identify this individual, an emergency disclosure, as per the Patriot Act, was instituted with [redacted] used by the individual who made the bomb threat.** By 7:00 a.m., a subject in [redacted] was identified. FBI [redacted] conducted a subject interview and the threat was determined to be non-credible by 11:00 a.m.

b2
b7E

[redacted] (S)

b1
b2
b7A
b7E

DATE: 12-03-2005
CLASSIFIED BY 61579DMH/LP/DFW
REASON: 1.4 ((c) 05-CV-0845)
DECLASSIFY ON: 12-03-2030

~~SECRET~~

Section 217 - INTERCEPTION OF COMPUTER TERSPASSER COMMUNICATIONS

b2
b6
b7A
b7C
b7E

Section 220 - NATIONWIDE SEARCH WARRANTS FOR ELECTRONIC EVIDENCE

b2
b6
b7A
b7C
b7E

~~SECRET~~

DATE: 09-20-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-20-2030

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 1:07 PM
To: [redacted] (OCA) (FBI)
Subject: FW: PATRIOT ACT Sunset Provisions

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted] (FBI)
Sent: Friday, March 25, 2005 1:04 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted] (FBI)
Subject: PATRIOT ACT Sunset Provisions

b2
b6
b7C
b7E

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted]

(S)

b1
b2
b7E

Point of Contact: [redacted]

b2
b6
b7C
b7E

~~UNCLASSIFIED~~

~~SECRET~~

~~UNCLASSIFIED~~

PATRIOT ACT
SUNSET PROVISIONS

CID EXAMPLES OF THE NEED FOR PATRIOT ACT SECTIONS 203 AND 218 (INFORMATION SHARING)

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist and foreign intelligence organizations and acts are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some of these examples which support the need for continued information sharing between criminal, counterterrorism and counterintelligence efforts are set forth below:

b2
b7A
b7E

A. Transnational Criminal Enterprises

1

Ongoing.

2.

b2
b7A
b7E

Ongoing.

3. Alien Smuggling

b2
b7E

b2
b7E

The following are examples of criminal intelligence developed and disseminated on alien smuggling matters:

b2
b6
b7A
b7C
b7E

a. FBI

b. FBI

b2
b7A
b7E

c.

d. FBI

b1
b2
b6
b7A
b7C
b7D
b7E

(S)

4.

b2 , b6, b7A, b7C, b7E

b2
b6
b7A
b7C
b7E

5. [redacted] Ongoing.

6. [redacted]

b2
b7E

7. [redacted]

b2
b7A
b7E

the arrest, indictment and subsequent deportation of the subjects from Hong Kong to [redacted] The charges included narcotics violations and providing material support to Al Qaeda.

8. [redacted] Ongoing.

b2
b6
b7A
b7C
b7E

9. [redacted]

b2
b7A
b7E

10. [redacted]

b2 , b7A, b7E

[redacted]

b2
b7E

[redacted] b2 b6 b7A b7C b7E

B. Americas Criminal Enterprises (drugs/gangs/major theft enterprises)

1. [redacted] (199M-[redacted]-280706) (281H-[redacted]-281341)

[redacted]

Investigation began as a Pentbomb lead concerning [redacted] in [redacted] was identified and determined to be a Taliban/Al Qaeda associate. He was a financial contributor to the Taliban and [redacted] where drug trafficking took place. He filed a fraudulent death claim for [redacted] with an insurance company and was convicted of mail fraud. One of his employees was located in [redacted] and deported after a drug conviction. b2 b6 b7C b7E

2. [redacted]

[redacted] b2 b7A b7E

3. [redacted] b2 b6 b7A b7C b7E

[redacted] Ongoing

4. [redacted]

[redacted] Ongoing. b2 b7A b7E

5. [redacted]

[redacted] Ongoing. b2 b6 b7A b7C b7E

b2
b7A
b7E

C. White Collar Crimes

1. Unlawful Redemption [ ] 265C [ ] 42132 [ ] 265F [ ] 282769)

b2
b6
b7A
b7E

[ ]

Ongoing.

2. [ ] b2 , b7A, b7E

b2
b6
b7A
b7C
b7E

[ ]

3 [ ] (272 [ ] 97082) b2 , b6, b7C, b7E

A drug/money laundering investigation identified subjects in Colombia, Spain, England and U.S., including a subject affiliated with the United Self-Defense Forces of Colombia (AUC), which is a recognized Foreign Terrorist Organization. Subject wants to purchase a bank in the U.S. to facilitate laundering of drug proceeds. Ongoing.

4. [ ] b2 , b7A, b7E

b2
b7A
b7E

[ ] Ongoing

5. Express Cleaners (272D [ ] 40807) b2 b7E

Investigation determined subjects were in position to launder millions through a location outside the U.S. through Lebanese and Saudi Arabian banks. The money would be returned to U.S. "clean" for a 20% fee. Two subjects identified had links to terrorists or terrorist activities.

b2 , b6, b7A, b7C, b7E

6. [ ]

[ ]

b2
b7A
b7E

b2 b6, b7C, b7E

7. [redacted]

[redacted]

b2
b6
b7A
b7C
b7E

8. [redacted] b2 , b6, b7C, b7E

[redacted]

[redacted] Ongoing. b2 , b6, b7A, b7C, b7E

b2
b7A
b7E

9. [redacted]

[redacted] (S)

b1
b2
b7A
b7E

10. [redacted] b2 , b6, b7A, b7C, b7E

[redacted]

[redacted] Ongoing.

b2
b6
b7A
b7C
b7E

11. [redacted] b2 , b6, b7A, b7C, b7E

[redacted]

b2
b7A
b7E

12. [redacted] b6 , b7A, b7C

[redacted]

b6
b7A
b7C

[redacted] b2 b7A b7D b7E

D. Public Corruption

1. [redacted] b2 , b7A, b7E

[redacted] b2 b7A b7D b7E

[redacted] Ongoing.

2. [redacted] b7A

[redacted] b2 b7A b7E

b2 b6 b7A b7C b7E

3. [redacted] 265B- [redacted] 42623, [redacted]

[redacted] b2 b6 b7A b7C b7E

Ongoing.

E. Civil Rights

1. Human Trafficking Investigations

Target organizations who traffic in aliens to be used as domestic servants, prostitutes and migrant workers. Investigations also develop foreign intelligence information.

PATRIOT ACT SUNSET PROVISIONS

CID EXAMPLES OF THE NEED FOR PATRIOT ACT SECTIONS 203 AND 218 (INFORMATION SHARING)

b5

b2

b5

In one such case, information from a criminal Title III and criminal investigation was passed to Counterterrorism, as well as and In another example, intelligence developed from criminal and counterintelligence investigations indicates foreign intelligence services and organized crime groups may be laundering billions of dollars through the U.S. banking system.

b2

b7E

In one instance, a terrorism case initiated in was subsequently transferred to and converted to a criminal case. The investigation focused on a group of individuals who were involved in arms trafficking, the production and

b2

b7E

distribution of multi-ton quantifies of hashish and heroin [redacted] The operation resulted in the arrest, indictment and subsequent deportation of the subjects from Hong Kong to [redacted] to face drug charges and charges of providing material support to Al Qaeda. b2 b7E

[redacted]

Criminal enterprises are also frequently involved in, allied with or otherwise rely on smuggling operations. Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens, smuggling anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and smuggling enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities. Current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts, has determined smugglers, as well as illegitimate and quasi-legitimate business operators in the United States, who use the services of illegal aliens, provide false travel documents to special interest aliens, deal with corrupt foreign officials, and financially support extremist organizations.

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Wednesday, March 16, 2005 5:31 PM
To: [redacted] (OCA) (FBI)
Subject: Patriot Act Examples

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] *Please review the following e-mail that I want to send to all ADICs/SACs.* [redacted] *Thanks.*

b5
b6
b7C

As the Director mentioned at the SAC Conference yesterday, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted]

b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Of particular interest are examples of Sections 203 and 218 (Information Sharing), 206 (Roving Wiretaps), 214 (FISA Pen Register and Trap/Trace), and 215 (Business Records).

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

Thank you for your assistance. Please contact me if you have any questions.

Eleni

UNCLASSIFIED

b2
b7E

PATRIOT ACT - SUNSET EXEMPLARS
FBI
(03/24/2005)

Sections 201 and 202 (Expanded Title III Predicates)

Nothing to report.

Sections 203 and 218 (Information Sharing)

(Pending)
CASE AGENTS:

b2
b6
b7A
b7C
b7E

Due to Patriot Act provisions, FBI shared Grand Jury information with This was very useful in

315M- -89387 (Pending)
AOT-IT
CASE AGENT:

b2
b6
b7C
b7E

Search warrants were prepared in Washington and served on Information obtained from search warrants, pen registers/trap traces, and Grand Jury Subpoena were shared with the United States Army and the Judge Advocate General for the Army. The same information was used in a Court Marshal in which was found guilty and sentenced to life in prison.

315N- -85481 (Closed)
(Pending)
IT-UBL/AL-QAEDA
CASE AGENT:

b2
b6
b7A
b7C
b7E

Section 203(d): Authorized sharing of criminal information with intelligence officials.

b2
b6
b7A
b7C
b7E

[redacted] (Pending)
[redacted]
CASE AGENT: [redacted]

Subject is under investigation [redacted] This investigation benefitted in general from the sharing of information across the intelligence/criminal investigation line. The break down of the so called "wall" between intelligence and criminal investigators resulted in the cross- sharing of information which supported and allowed for the use of investigative techniques, to include, [redacted]

b2
b6
b7C
b7E

The [redacted] investigation generated numerous leads to other divisions and the initiation of preliminary inquiries and full field investigations on related subjects. In addition, several Legal Attaches were tasked with sharing information via Letterhead Memorandum and further tasked for foreign records checks and interviews.

Section 204 (Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications)

315N-[redacted]-85481 (Closed)
[redacted] (Pending)
[redacted]
IT-UBL/AL-QAEDA
CASE AGENT: [redacted]

b2
b5
b6

This section granted FBI [redacted] use of FISA for [redacted] of [redacted] as well as search of stored [redacted]

b7A
b7C
b7E

Section 206 (Roving Wiretaps)

[redacted] (Pending)
CASE AGENT: [redacted]

Roving authority applied for and received under a newly issued FISA.

b2
b6
b7A
b7C
b7E

Section 213 (Delayed Notice Search Warrants)

[redacted](Pending)
CASE AGENT: [redacted]

FBI [redacted] applied for and received a Delayed Notice Search Warrant in captioned case. The search has not yet taken place, however, it is anticipated significant information will be recovered.

Section 214 (FISA Pen Register and Trap/Trace)

315N-[redacted]-85481 (Closed)
[redacted](Pending)
[redacted]
IT-UBL/AL-QAEDA
CASE AGENT: [redacted]

Section 214 allowed FISA pen/trap authority based upon the fact information obtained was likely to result in foreign intelligence information. [redacted] and provided valuable intelligence information regarding the subject, suspect organization [redacted] and terrorism related matters.

Section 215 (Business Records)

FBI [redacted] is considering use of this provision in the near future in two separate foreign counterintelligence investigations in order to obtain business records on two subjects of interest. However, due to the classified nature of these investigations further details are unavailable at this time.

Section 217 (Computer Hacking victims requesting law enforcement assistance)

288A-[redacted]90406 (Pending)
UNSUB(S);
[redacted]
COMPUTER INTRUSION
CASE AGENT: [redacted]

This section of the Patriot Act was vital to this investigation. FBI [redacted] Case Agent was able to locate [redacted] If not for this exception, the Case Agent would

have been unable to gather critical information.

Section 218 (Change in the "Primary Purpose" Standard of FISA)

315N-[redacted]-85481 (Closed)
[redacted] (Pending)
[redacted]
IT-UBL/AL-QAEDA
CASE AGENT: [redacted]

This section eliminated the wall and allowed for sharing of criminal and intelligence information. It also allowed FBI [redacted] to coordinate with cleared law enforcement officials assigned to the [redacted]JTTF and prosecutors from the U.S. Attorney's Offices (USAOs) both in [redacted] (where [redacted] was indicted) and [redacted]

This section also enabled the sharing of information with cleared law enforcement personnel needed to effect arrests and other investigative actions (surveillance, etc.) It enabled criminal investigators to share Grand Jury information with other law enforcement entities working both on the intelligence and criminal sides of the investigation. This was vital to the case as 100's of Grand Jury subpoenas were issued and provided cause documents for [redacted] search, and arrest warrants.

b2
b6
b7A
b7C
b7E

Finally, this section paved the way for use of FISA derived material in [redacted] prosecution and in [redacted] proceedings, once said material was properly declassified. This section was vital to FBI [redacted] sharing with numerous other field divisions working on investigations related to the [redacted] matter to include: [redacted] and [redacted] Some of the intelligence derived from the FBI [redacted] investigation [redacted] has proven beneficial to intelligence and/or criminal cases out of the following Divisions: [redacted] and others.

Section 220 (Nationwide Search Warrants for Electronic Evidence)

[redacted] (Pending)
[redacted] (Victim)
[redacted]
CASE AGENT: [redacted]

b2
b6
b7A
b7C
b7E

[redacted] was arrested in February 2005. A search warrant sworn out in [redacted] was served on [redacted] The resulting information will be used in the prosecution of [redacted]

b2
b5
b6
b7A
b7C
b7E

[redacted] (Pending)

CASE AGENT: [redacted]

[redacted] A search warrant was sworn out in [redacted] and served in [redacted] on [redacted] The information obtained through this warrant contains evidence of [redacted] use of the internet to [redacted]

b2
b5
b6
b7A
b7C
b7E

315M-[redacted]-89387 (Pending)

[redacted]

AOT-IT

CASE AGENT: [redacted]

[redacted] Search warrants were prepared in [redacted] and served on [redacted] Information obtained from search warrants, pen registers/trap traces, and Grand Jury Subpoenas were shared with the United States Army and the Judge Advocate General for the Army. The same information was used in a Court Marshal in which [redacted] was found guilty and sentenced to life in prison.

b2
b6
b7C
b7E

315N-[redacted]-85481 (Closed)

[redacted] (Pending)

[redacted]

IT-UBL/AL-QAEDA

CASE AGENT: [redacted]

This section enabled search warrants from the FISA court to compel [redacted] located in [redacted] to provide stored content.

b2
b6
b7A
b7C
b7E

Section 225 (Immunity for Compliance with FISA Wiretap)

315N-[redacted]-85481 (Closed)

[redacted] (Pending)

[redacted]

IT-UBL/AL-QAEDA

CASE AGENT: [redacted]

b2
b6
b7A
b7C
b7E

This section provided immunity to [redacted] and [redacted] personnel [redacted] content was utilized throughout the criminal proceedings against [redacted]

b2
b6
b7A
b7C
b7E

Administrative Suggestions:

[redacted]

[redacted]

b2
b5
b7E

[redacted]

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 12:42 PM
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples

b6
b7C

Importance: High

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-29-2005 BY 65179 DMH / JHF 05-CV-0845

UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted](FBI)
Sent: Friday, March 25, 2005 12:24 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI); [redacted](FBI)
Subject: FW: Patriot Act Examples
Importance: High

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Example of use of these provisions in a [redacted]Division criminal case is attached.

-----Original Message-----
From: [redacted](FBI)
Sent: Monday, March 21, 2005 2:48 PM
To: [redacted](FBI); [redacted](FBI); [redacted](FBI)
Subject: FW: Patriot Act Examples
Importance: High

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Lets see if we can get some examples.

[redacted]

b6
b7C

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted]

[redacted]

b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] b2 , b6, b7A, b7C, b7E

(1) Section 212 -amended 18 U.S.C. § 2702(b); § 220 - amended 18 U.S.C. § 2703.

Sections 212 and 220 of the PATRIOT Act were utilized [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

b2
b6
b7A
b7C
b7E

Section 220 was used to obtain search warrants for [redacted]

[redacted]

b6
b7A
b7C

[redacted] eventually pled guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor (18 U.S.C. §§ 2423(b) and 2251(a)) and was thereafter sentenced to a term of 235 months imprisonment.

From: [redacted] OGC) (FBI)
Sent: Friday, March 25, 2005 1:03 PM
To: [redacted] (CTD) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (FBI); [redacted] (OGC) (FBI); [redacted] (OCA) (FBI)
Subject: RE: Quick question on FBI Director testimony for Congress on FISA issue relating to [redacted]

UNCLASSIFIED
NON-RECORD

I see no issue with this. As written below, it is accurate. In addition, there is no way that anyone could glean what investigation and/or prosecution this refers to.

-----Original Message-----
From: [redacted] CTD) (FBI)
Sent: Friday, March 25, 2005 12:59 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (FBI); [redacted] (OGC) (FBI); [redacted] (OCA) (FBI)
Subject: RE: Quick question on FBI Director testimony for Congress on FISA issue relating to [redacted]

UNCLASSIFIED
NON-RECORD

[redacted]
I just got this from Office of Congressional Affairs. They queried field offices, to include [redacted], for examples of FISAs that utilize Patriot Act, Section 204. The [redacted] case came up as an example. SA [redacted] provided below response - below the asterisks - which looks VERY generic. Probably no issues here but thought I would cut you in to take a quick read. Let [redacted] and myself know if you see any problem with this. Thanks.

-----Original Message-----
From: [redacted] (FBI)
Sent: Friday, March 25, 2005 12:03 PM
To: [redacted] CTD) (FBI)
Subject: FW: Patriot Act Example

UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted] FBI)
Sent: Friday, March 25, 2005 11:56 AM
To: [redacted] (FBI); [redacted] (FBI)
Subject: RE: Patriot Act Example

UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

[redacted] b2 b6 b7C b7E

-----Original Message-----
From: [redacted](FBI) b2 b6 b7C b7E
Sent: Friday, March 25, 2005 10:50 AM
To: [redacted](FBI); [redacted](FBI)
Subject: FW: Patriot Act Example

DATE: 12-08-2005
CLASSIFIED BY 65179 DMH/LP/DFW
REASON: 1.4 ((C) 05-CV-0845)
DECLASSIFY ON: 12-08-2030

UNCLASSIFIED
NON-RECORD

Guys:

This is the email regarding the Patriot Act and the Congressional Affairs call I received today.

Can we all get together on this to make sure we are comfortable with it?

[redacted] b6 b7C

-----Original Message-----
From: [redacted](OCA) (FBI)
Sent: Friday, March 25, 2005 10:17 AM
To: [redacted](FBI); [redacted]FBI)
Subject: Patriot Act Example b2 b6 b7C b7E

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted]- thanks very much for your help this morning. [redacted]

[redacted] b5 b6

[redacted]- thanks for your help! b7C

****

[redacted] b1 b2 b7E

(S)

[redacted]
Office of Congressional Affairs
[redacted] b2 b6 b7C

UNCLASSIFIED

~~SECRET~~

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

From: KALISCH, ELENI P. (OCA) (FBI) b6
Sent: Monday, March 28, 2005 7:42 AM b7C
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act Examples

Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

-----Original Message-----
From: [redacted] (FBI) b2
Sent: Sunday, March 27, 2005 2:15 PM b6
To: KALISCH, ELENI P. (OCA) (FBI) b7C
Cc: [redacted] (FBI); [redacted] (FBI) b7E
Subject: FW: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

(S) b2 b6 b7C b7E

Hi Eleni,
I am the [redacted] and am the the POC for this. Set forth below is an e-mail which I sent to all SAs soliciting further examples. As a a result of response from SAs, I have the additional information.

Sections 201 and 202 [redacted] b1 , b2, b7E

Section 203 - [redacted] ed this in all of our 315 investigation. It is difficult to quantify the extent to which we have made use of this. b2 b7E

Section 218 - Again, this is difficult to quantify, but since the enactment of the Patriot Act we have utilized a FISA on approximately [redacted] T investigations. The "significant purpose" language was utilized in each of these.

(S)

Section 206 - I believe this has been used [redacted] on 315 investigations.

(S)

Section 214 - The pen register FISA has been used approximately [redacted] (S) b1 b2 b7E

Section 215 - [redacted] (S)

Section 217 - (S)

Section 213 - We have had [redacted] search warrant in a criminal investigation. We reported this previously about 2 years ago we when we executed the warrant.

Please contact me if you need more information.

[redacted]

-----Original Message-----
From: [redacted] (FBI) b2
Sent: Thursday, March 17, 2005 5:43 PM b6
To: [redacted] SUPERVISORS; [redacted] ALL AGENTS b7C
Cc: [redacted] (FBI) b7E
Subject: FW: Patriot Act Examples
Importance: High

SECRET

~~UNCLASSIFIED~~
~~NON-RECORD~~

To follow up on the SAC's earlier e-mail to all supervisors which is set forth below and which requests examples of investigations which might be useful in convincing Congress to renew sections of the Patriot Act which are scheduled to expire at the end of this year, the following sections appear to be most relevant:

Sections 202 and 202 which expand the criminal Title 3 predicates to include some additional terrorism statutes and some computer fraud/hacking crimes [redacted] (the child pornography T-3 from a few years ago does not fall within this) (S)

b1
b2
b7E

Sections 203 which expands the sharing of information information obtained in criminal investigations, Grand Juries, and Title 3s with other federal intelligence or law enforcement agency to the extent the information relates to national security [redacted] **Any specific examples where we achieved some notable result should be reported to me.** (S)

Section 218 - This section amended the FISA statute to allow for foreign intelligence to be a "significant purpose" of the authority sought. In conjunction with section 504, this also allows us to consult with federal prosecutors without placing FISAs at risk. Since this applies to all FISAs obtained since 10/26/01, I will obtain the number of these we have had since that time.

b1
b2
b7E

Section 206 - roving FISA coverage which authorizes interception of facilities as yet unknown if the subject's actions may thwart electronic surveillance. I recall that this has been used [redacted] on a Squad 4 case, but do not recall other instances. **Please advise me if we have used on other occasions.** (S)

Section 214 - FISA pen register and trap/trace - This change modified the standard for obtaining FISA pen registers and added required language relating to the 1st Amendment - I will get the responsive numbers for this from ELSUR

Section 215 - FISA for business records - [redacted] **Please advise me if we have used this technique.** (S)

b1
b2
b7E

Section 217 - law enforcement monitoring of computer trespassers - This section is a technical amendment to the computer hacking statute and allows us to conduct electronic surveillance of the intruder with the consent of owner of the computer system. [redacted] **Please advise me of any situations where this has been used.** (S) (S)

Section 213 - delayed notice criminal search warrants - [redacted] on a drug investigation; and it was reported previously and was included in materials previously reported to Congress. **Any other examples should be brought to my attention.**

Any information regarding these should be forwarded to me as soon as possible, and any questions should be directed to me.

-----Original Message-----
From: [redacted] (FBI)
Sent: Thursday, March 17, 2005 10:54 AM
To: [redacted] SRAs; [redacted] SUPERVISORS
Cc: [redacted] (FBI)
Subject: FW: Patriot Act Examples
Importance: High

b2
b6
b7C
b7E

~~UNCLASSIFIED~~
~~NON-RECORD~~

~~SECRET~~

Please assist [redacted] in coordinating a response for this important matter.

b6
b7C

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 9:07 AM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

UNCLASSIFIED

SECRET

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 4:49 PM
To: [redacted] (OCA) (FBI) b6 b7C
Subject: FW: Patriot Act Examples

Importance: High

DATE: 09-20-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-20-2030

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

[redacted] will fit right in. b6 b7C

-----Original Message-----
From: [redacted] (FBI) b2 b6 b7C b7E
Sent: Friday, March 25, 2005 4:12 PM
To: KALISCH, ELENI P. (OCA) (FBI); [redacted] (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Eleni- Here is the response from [redacted] I think it is important to note that , even though our realitivly small division has not used all the tools provided by the Patriot Act, it is important to have those tools available to us. [redacted] points of contact are SSA [redacted] SSA [redacted] and/or [redacted] b2 b6 b7C b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Tuesday, March 22, 2005 9:30 AM
To: [redacted] (FBI)
Subject: FW: Patriot Act Examples
Importance: High

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

[redacted] Here is the CI-1 response regarding the Patriot Act sunset provisions:

[redacted] (S) b1 b2 b5 b6 b7C b7E

SECRET

I hope that all makes cents (opps sense). [redacted] b6 b7C
-----Original Message-----
From: [redacted] (FBI)
Sent: Thursday, March 17, 2005 12:36 PM
To: [redacted] (FBI); [redacted] (FBI) [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI) [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI) [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] (FBI) b2 b6 b7C b7E
Subject: FW: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

If you have any example, let [redacted] know by 3/23/2005.

b6 b7C

[redacted] - Please coordinate our division's response and note 3/25/2005 deadline to FBIHQ..

[redacted] b2 , b7E
-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 10:07 AM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

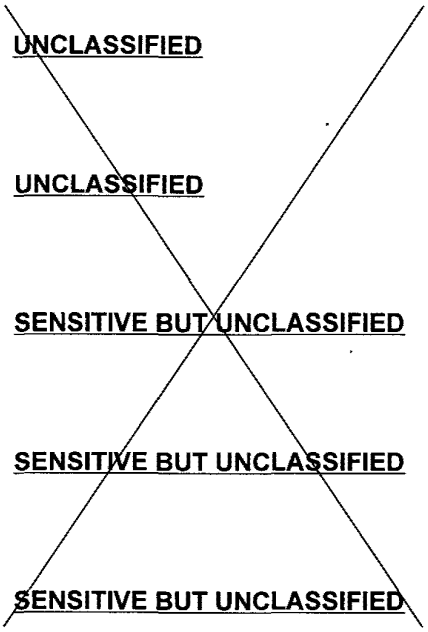
Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni



SECRET

PATRIOT ACT Provision: Section 217
CASE Example: Major Case (MC) 216

Discussion: Investigation identified a computer intruder who used a series of intermediary computers as an initiating point of subsequent attacks against a main target. The captioned provision allowed the FBI to contact the victim of an intermediary attack and request that the victim company or individual create a record of activity. Further, the FBI could obtain consent from the intermediary victim and monitor criminal activity contemporaniously.

PATRIOT ACT Provision: Section 206
CASE Example: Various

Discussion: Investigations using Title 50 and Title III intercept and search authority have determined that subjects use multiple accounts. The current process requires multiple orders or subsequent orders. Implementation of the "roving" provision of Section 206 would reduce redundant orders and unnecessary delay in monitoring previosuly unknown accounts.

From: KALISCH, ELENI P. (OCA) (FBI) b6
Sent: Friday, March 25, 2005 12:44 PM b7C
To: [redacted] (OCA) (FBI)
Subject: FW: PATRIOT ACT Sunset Provisions

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-29-2005 BY 65179 DMH/JHF 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted] (FBI) b2
Sent: Friday, March 25, 2005 12:44 PM b6
To: KALISCH, ELENI P. (OCA) (FBI) b7C
Cc: [redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] b7E
[redacted] (FBI); [redacted] (FBI); [redacted] (FBI); [redacted] FBI)
Subject: PATRIOT ACT Sunset Provisions

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
Reference: Electronic Mail communication between receiver and ASAC [redacted] dated, 03/17/2005, Subject: b7C
"PATRIOT ACT Examples"

Ms Kalisch,

b6
[redacted] asked that I forward to you our best, substantive, examples of PATRIOT ACT as a response to the b7C
above referenced communication.

In [redacted] we conduct hundreds of information sharing examples through our JTTF partners everyday. It is daily business for us to properly disseminate information in accordance the sections allowing dissemination of b2
FGJ and other information. b7E

The examples attached are specific to our cyber-counterterror experience in [redacted] Please contact me for further clarification or elucidation.

Best Regards, b2
SA [redacted] b6
[redacted] b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Wednesday, March 23, 2005 5:25 PM
To: [redacted](OCA) (FBI)
Subject: FW: Patriot Act Examples

b6
b7C

Importance: High

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-29-2005 BY 65179 DMH/JHF 05-CV-0845

-----Original Message-----
From: [redacted](FBI)
Sent: Wednesday, March 23, 2005 5:11 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted](FBI); [redacted]FBI); [redacted](FBI); [redacted](FBI)
Subject: FW: Patriot Act Examples
Importance: High

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Eleni:

Attached is the [redacted] Division response to your request. Individual examples contain the name of the case agents who will be able to assist you if further information is required. However, you may also contact [redacted] or IA [redacted] if you require further assistance.

b2
b6
b7C
b7E

Enjoy your day.

IA [redacted]
[redacted] Division
[redacted]

b2
b6
b7C
b7E

-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 9:07 AM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted]

b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday,

March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

b6
b7C

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 5:25 PM
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act

DATE: 09-21-2005
CLASSIFIED BY 60309 AUC TAM/MLT/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-21-2030

~~UNCLASSIFIED~~
~~NON-RECORD~~

-----Original Message-----
From: [redacted] (FBI)
Sent: Friday, March 25, 2005 5:14 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Cc: [redacted] (FBI)
Subject: Patriot Act

b2
b6
b7C
b7E

~~UNCLASSIFIED~~
~~NON-RECORD~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2
b7E

On behalf of the [redacted] Division SAC, here is the [redacted] Division response to your Patriot Act request:

Section 201/202 (TIII predicates)

The [redacted] Division [redacted] the expanded predicates to obtain a Title III. (S) b1 , b2, b7E

Section 203 (Information Sharing)

(S)

[redacted] b1 b2 b5 b7E

Section 218 (FISA)

[redacted] b2 b5 b7E

Section 206 (Roving Wiretaps)

(S)

The [redacted] the roving wiretap authority under this section. b1 b2 b7E

Section 214 (FISA Pen/Trap)

[redacted] b1 b2 b7E

Some of the Pen/Traps may have not risen to the level of justification required under the old standard. In addition, the [redacted] has utilized the expanded "electronic communications" portion of this section. [redacted] has obtained a FISA pen/trap in [redacted] involving electronic communications, with a total of [redacted] including the renewal orders. (S)

Section 215 (Business Records)

[redacted] recently submitted [redacted] FISA Business Records request in an FCI investigation, but has not yet (S) b1 b2 b7E

SECRET

received the results of the request. This Business Records request would not have met the pre-Patriot Act standards and would have been unavailable without this section.

Section 217 (Computer Hacking)

[redacted] b2 b5 b7A b7E

If you need any additional information Eleni, do not hesitate to call.

[redacted] b2 b6 b7C b7E

~~UNCLASSIFIED~~
~~NON-RECORD~~

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

~~UNCLASSIFIED~~

~~UNCLASSIFIED~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 09-21-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 09-21-2030

b2
b7E

PATRIOT ACT EXAMPLES RELATED TO SUNSET PROVISIONS
FBI [ ] DIVISION

(S)

Sections 201 and 202 (Expanded Title III predicates)

[ ] examples

Sections 203(b) and (d) (Information Sharing)

(S) [ ] examples

Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

[ ] examples

(S) Section 206 (Roving Wiretaps)

b1
b2
b7E

[ ] examples

(S) Section 207 - Extended Duration for Certain FISAs

[ ] examples

(S) Section 209 - Seizure of Voice Mail with a Search Warrant

[ ] examples

(S) Section 212 - Emergency Disclosures of E-mail & Records by ISPs

[ ]

b2
b6
b7A
b7C
b7E

Section 214 (FISA Pen Register and Trap/Trace)

FISA pen register and trap/trace authority has been used [ ]

[ ]

b2
b7E

[redacted] b2 b5 b7E

Section 215 (Business Records)

[redacted] examples (S) b1 b2 b7E

Section 217 - Interception of Computer Trespasser Communications

The following examples are of occasions during which victims invited the FBI into a protected computer to monitor a computer trespasser's communications:

1) [redacted] b2 b6 b7A b7C b7E

2) The victim in a criminal computer intrusion case allowed consensual real-time monitoring of his home network in an attempt to intercept the subject intruder's online activity (data). As it turned out, the subject never returned and connected to the victim wireless network, but the FBI did eventually search and seize computers from both the subject's vehicle and residence.

3) [redacted] b2 b7A b7E

b2
b7A
b7E

Section 218 (Change of Primary Purpose/Information Sharing)
Following are two examples of cases in which personnel involved in a FISA consulted with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities. This was accomplished because the "wall" between criminal and intelligence investigations was eliminated. These examples are being provided as they may relate to the change in the purpose standard for FISA authority:

1)

b1
b2
b7E

Impact of the Patriot Act:

During a national press conference on the day of the indictment and arrests of the subjects of this case, then Attorney General John Ashcroft described this case as a landmark investigation and prosecution. Former Attorney General Ashcroft also heralded [redacted] and RICO prosecution as a new method of attacking terrorism following the passage of the Patriot Act. b2 b7E

2) In a pending international terrorism case, the FBI has been able to coordinate with ICE and with local intelligence officers in an effort to arrest/detain an international terrorism subject for eventual deportation. This case involves ongoing declassification of FISA derived information to be used in the criminal case. The change in the purpose for the FISA authority has allowed coordination between the criminal and intelligence investigations in this case.

Section 220 - Nationwide Search Warrants for Electronic Evidence

The FBI has used Section 220 in numerous innocent images criminal cases to obtain search warrants with nationwide jurisdiction to compel the production of information held by service providers in other districts or states. The information acquired from these nationwide search warrants provided evidence that the subjects were in possession of child pornography. On at least one occasion, a judge repeatedly refused to sign the nationwide search warrant because he believed this provision only applied to terrorism related matters. Ultimately, however, the FBI obtained the search warrant in this case from another judge.

Section 223 - Civil Liability for Certain Unauthorized Disclosures

[redacted] examples (S)

Section 225 - Immunity for Compliance with FISA Wiretap

[redacted] examples (S) b1 b2 b7E

Section 213 (Delayed Notice Search Warrants)--Not subject to sunset

[redacted] examples (S)

From: [redacted] (DO) (FBI)
Sent: Friday, March 25, 2005 2:19 PM
To [redacted] OCA) (FBI)
Subject: FW: [redacted] Division's Response Re: Patriot Act Examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-29-2005 BY 65179 DMH /JHF 05-CV-0845

FYI...

-----Original Message-----
From: [redacted] FBI)
Sent: Friday, March 25, 2005 2:18 PM
To: KALISCH, ELENI P. (OCA) (FBI); [redacted] (DO) (FBI)
Cc: [redacted] (FBI); [redacted] (FBI)
Subject: [redacted] Division's Response Re: Patriot Act Examples

b2
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

Please find attached [redacted] Division's response to the e-mail dated 03/17/2005, requesting submission of unclassified examples of the Division's use of Patriot Act provisions.

[redacted] point of contact (POC) for additional information is [redacted] telephone number [redacted]

b2
b6
b7C
b7E

Approved By:
[redacted]

Sent By:
[redacted]

[redacted] Legal Unit
[redacted]

b2
b6
b7C
b7E

UNCLASSIFIED

UNCLASSIFIED

b6

b7C

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Friday, March 25, 2005 2:53 PM
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act Examples

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: Caproni, Valerie E. (OGC) (FBI)
Sent: Friday, March 25, 2005 2:51 PM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: FW: Patriot Act Examples

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I think this is in response to a tasking from you.

-----Original Message-----
From: BEREZNAY, TIMOTHY D. (CD) (FBI)
Sent: Friday, March 25, 2005 2:48 PM
To: Caproni, Valerie E. (OGC) (FBI)
Subject: FW: Patriot Act Examples

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: GUERIN, RONALD T. (CD) (FBI)
Sent: Thursday, March 24, 2005 8:49 AM
To: BEREZNAY, TIMOTHY D. (CD) (FBI)
Subject: FW: Patriot Act Examples

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

If you need more specifics let me know.
-----Original Message-----
From: [redacted] (CD) (FBI)
Sent: Wednesday, March 23, 2005 1:44 PM
To: GUERIN, RONALD T. (CD) (FBI)
Subject: RE: Patriot Act Examples

b6

b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Rudy,

One addition for 3A:

b2
b7E

[redacted]

-----Original Message-----
From: [redacted] (CD) (FBI)
Sent: Wednesday, March 23, 2005 1:26 PM
To: GUERIN, RONALD T. (CD) (FBI)
Cc: [redacted] (CD) (FBI)
Subject: RE: Patriot Act Examples

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Rudy,

CD-3A response:

[redacted]

b2
b7E

[redacted]

-----Original Message-----
From: [redacted] (CD) (FBI)
Sent: Monday, March 21, 2005 11:00 AM
To: [redacted] (INSD) (FBI); [redacted] (CD) (FBI) [redacted] CD) (FBI); [redacted] (CD) (FBI); [redacted] (SecD) (FBI)
Cc [redacted] (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

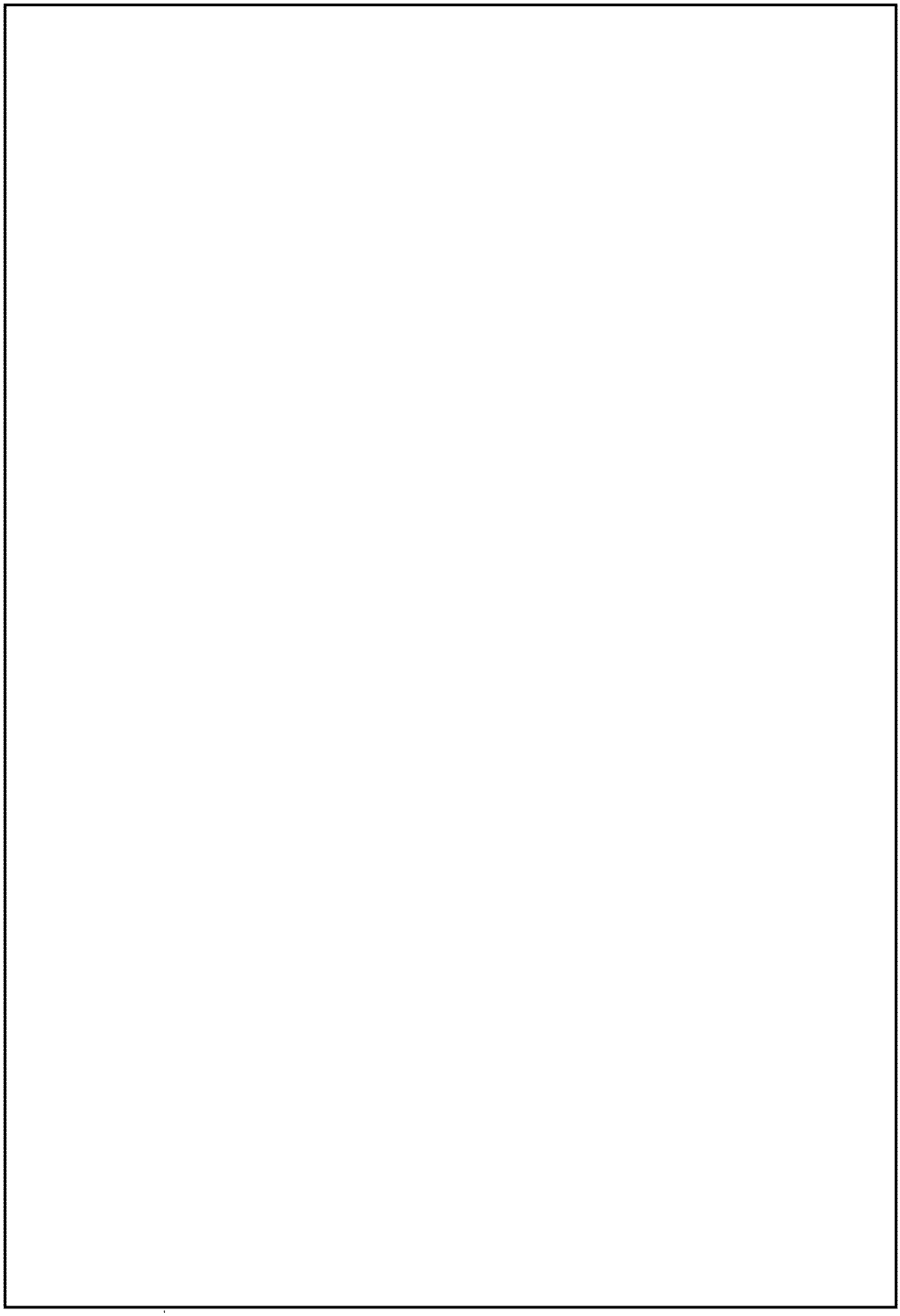
b6
b7C

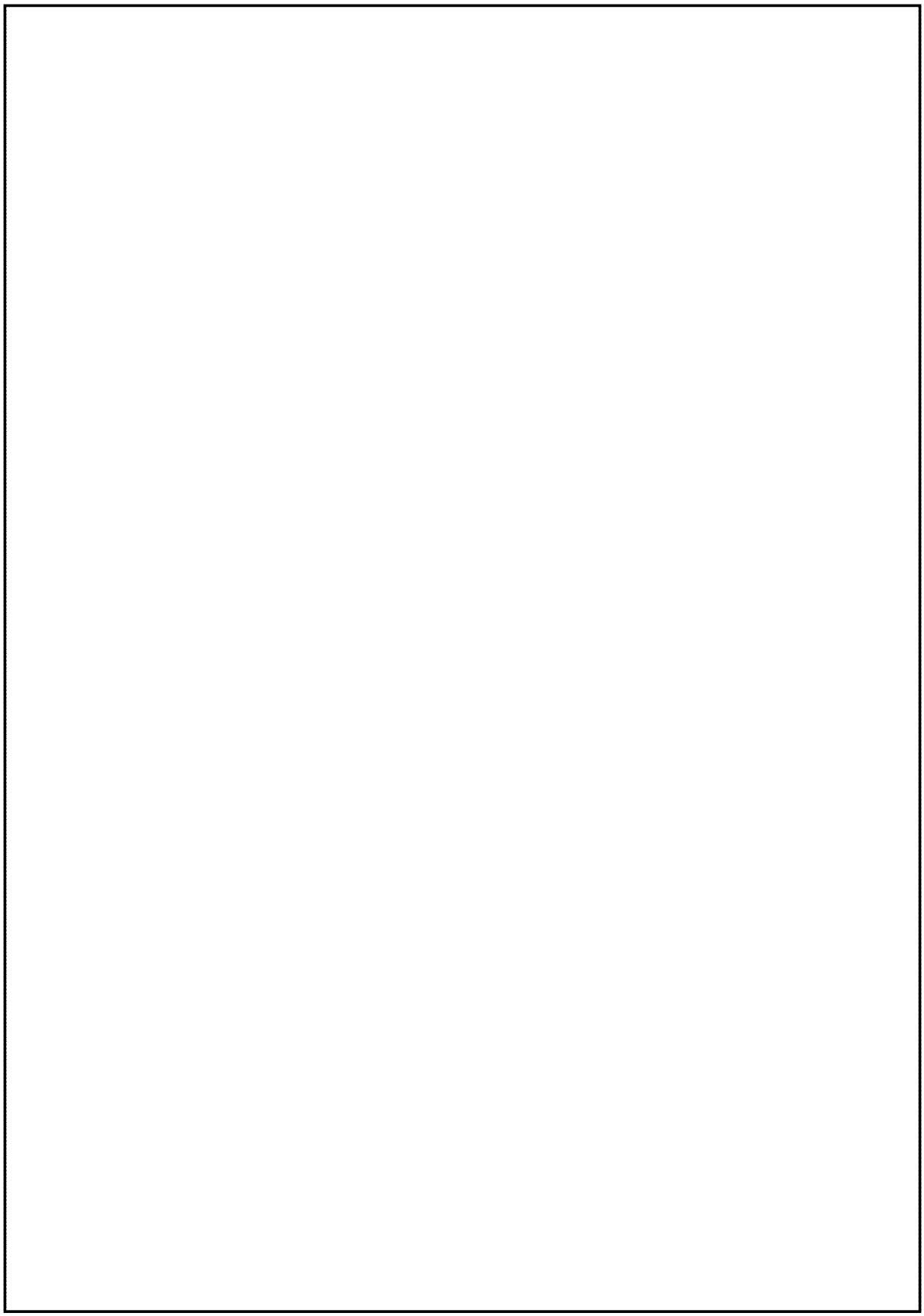
UNCLASSIFIED
NON-RECORD

Per Rudy's request below, we've been asked to review the below identified sections of the USAPATRIOT act that are scheduled to be sunsetted this year. OCA wants to know whether FBI has used these sections. Many of the sections exanded upon Title III wiretaps, but several of the sections may have impacted 3A cases such as Sections 206, 207, and 214. Can we identify any cases or circumstances in which we've used one or more of these sections? If so, email Rudy, no later than Thursday, unclassified versions of such examples.

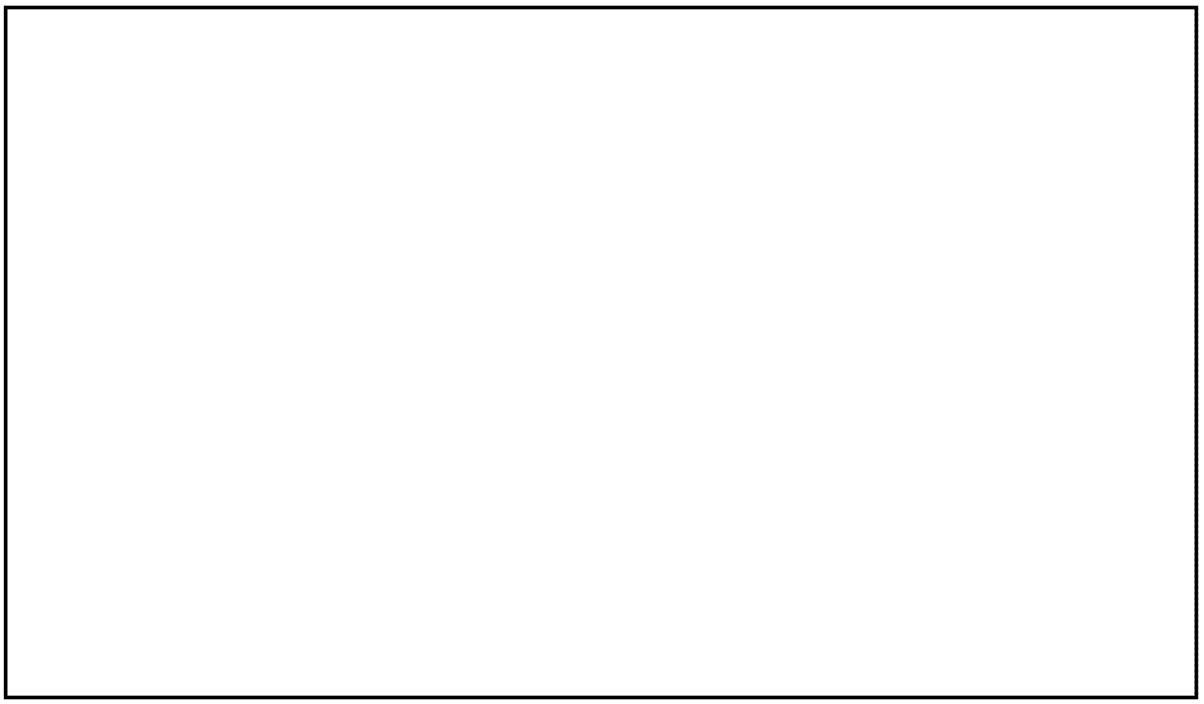
[redacted]

b5





b5



-----Original Message-----
From: GUERIN, RONALD T. (CD) (FBI)
Sent: Monday, March 21, 2005 10:43 AM
To: [redacted](CD) (FBI); [redacted](CD) (FBI); [redacted](CD) (FBI); [redacted](CD) (FBI); [redacted](CD) (FBI); [redacted](CD) (FBI); [redacted](CD) (FBI); [redacted](CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

Any examples where we utilized the provisions of the Patriot Act? I know in 3D we have several, but we might have others as well. Note the deadline.
-----Original Message-----
From: BEREZNAY, TIMOTHY D. (CD) (FBI)
Sent: Monday, March 21, 2005 10:19 AM
To: DONNER, MICHAEL A. (CD) (FBI); DESLAURIERS, RICHARD (CD) (FBI); GUERIN, RONALD T. (CD) (FBI); FAVREAU, KEVIN (CD) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

Pls canvas your troops and provide examples to me by noon Thursday.
-----Original Message-----
From: SZADY, DAVID (CD) (FBI)
Sent: Monday, March 21, 2005 8:01 AM
To: BEREZNAY, TIMOTHY D. (CD) (FBI); ANDRESS, BEVERLY (CD) (FBI)

Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

I know we have wxamples such as Rudy's [redacted] b2
-----Original Message----- b7E
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

b6
b7C

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:11 PM
To: [redacted] (OCA) (FBI)
Subject: FW: Patriot Act Benefits to [redacted] Investigation

SENSITIVE BUT UNCLASSIFIED b2 , b7A, b7E
RECORD [redacted]

[redacted]

I have sent out my All SACs e-mail and will forward responses to you. Here is the first :-) b6
Thanks, b7C
Eleni

b2
b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Thursday, March 17, 2005 11:55 AM
To: KALISCH, ELENI P. (OCA) (FBI)
Subject: FW: Patriot Act Benefits to [redacted] Investigation

SENSITIVE BUT UNCLASSIFIED b2 , b7A, b7E
RECORD [redacted]

Eleni,

Are you need of the below information?

[redacted]

b2
b6
b7C
b7E

[redacted]
ASAC CTD [redacted]
[redacted]

-----Original Message-----
From: PARENTI, DREW S (DO) (FBI)
Sent: Thursday, March 17, 2005 11:50 AM
To: [redacted] (FBI)
Subject: RE: Patriot Act Benefits to [redacted] Investigation

SENSITIVE BUT UNCLASSIFIED b2 , b7A, b7E
RECORD [redacted]

Not sure where that came form. The AD of OCA, Eleni Kalisch, is compiling specific examples of where the "sunsetting" provisions of the Patriot Act have assisted our investigations.

-Drew-

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Thursday, March 17, 2005 11:43 AM
To: PARENTI, DREW S (DO) (FBI)
Subject: FW: Patriot Act Benefits to [redacted] Investigation

SENSITIVE BUT UNCLASSIFIED b2 , b7A, b7E
RECORD [redacted]

Drew,

In the ADIC's morning meeting there was discussion that you were putting together talking points for the Director ref the Patriot Act. Please see below and let me know if this helps. Feel free to have a direct conversation with either [redacted] or [redacted] if it will benefit your research. Thanks

b2
b6
b7C
b7E

[redacted]

[redacted]
ASAC CTD [redacted]
[redacted]

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Thursday, March 17, 2005 11:17 AM
To: [redacted] (FBI)
Subject: FW: Patriot Act Benefits to [redacted] Investigation

b2 , b7A, b7E

SENSITIVE BUT UNCLASSIFIED
RECORD [redacted]

[redacted]

Here are the bullet points you requested.

b2
b6
b7C
b7E

-----Original Message-----
From: [redacted] (FBI)
Sent: Thursday, March 17, 2005 10:21 AM
To: [redacted] (FBI)
Cc: [redacted] (FBI)
Subject: Patriot Act Benefits to [redacted] Investigation

b2 , b7A, b7E

SENSITIVE BUT UNCLASSIFIED
RECORD [redacted]

[redacted]

b2
b5
b6
b7A
b7C
b7E

SA [redacted]
IT-3
(Desk) [redacted]
(Cell)

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

U.S. Department of Justice
Federal Bureau of Investigation

Office of Public and Congressional Affairs

Director 5/20/04
SJC Hearing

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE HEARING

NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?

b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

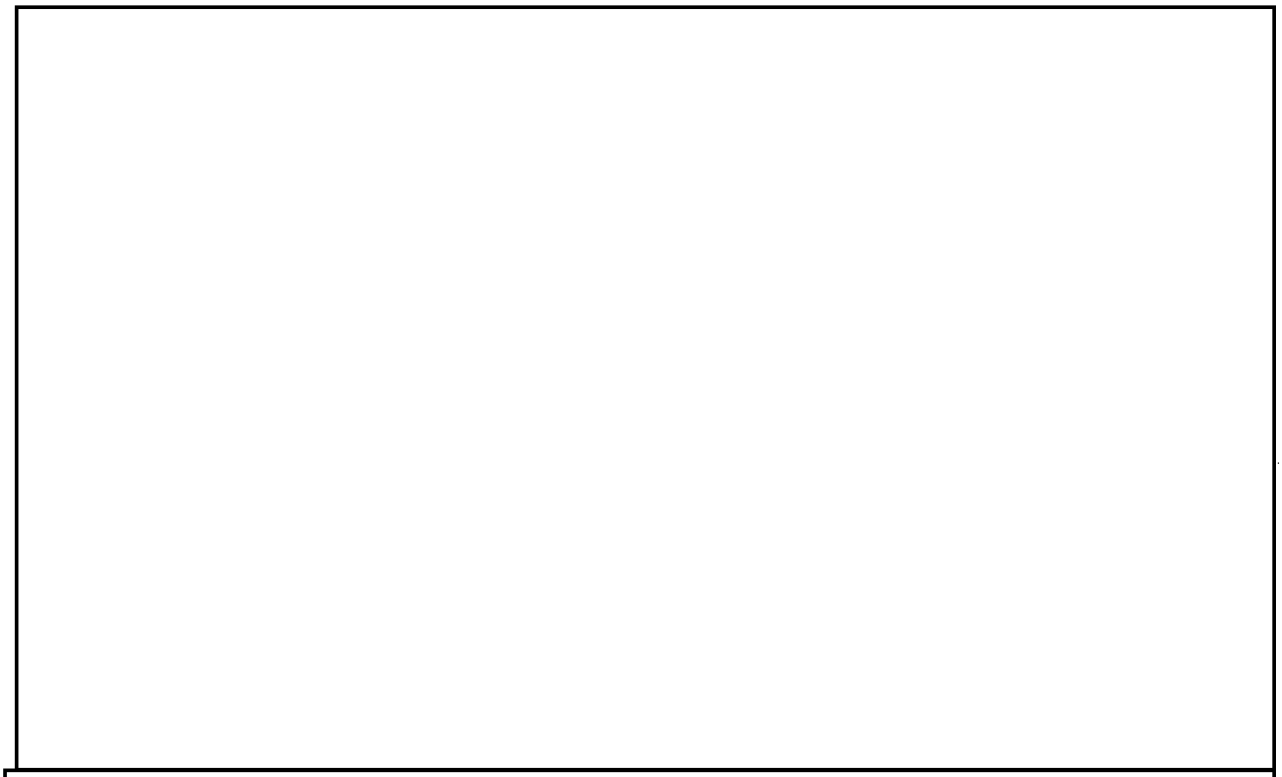
Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors.

b5

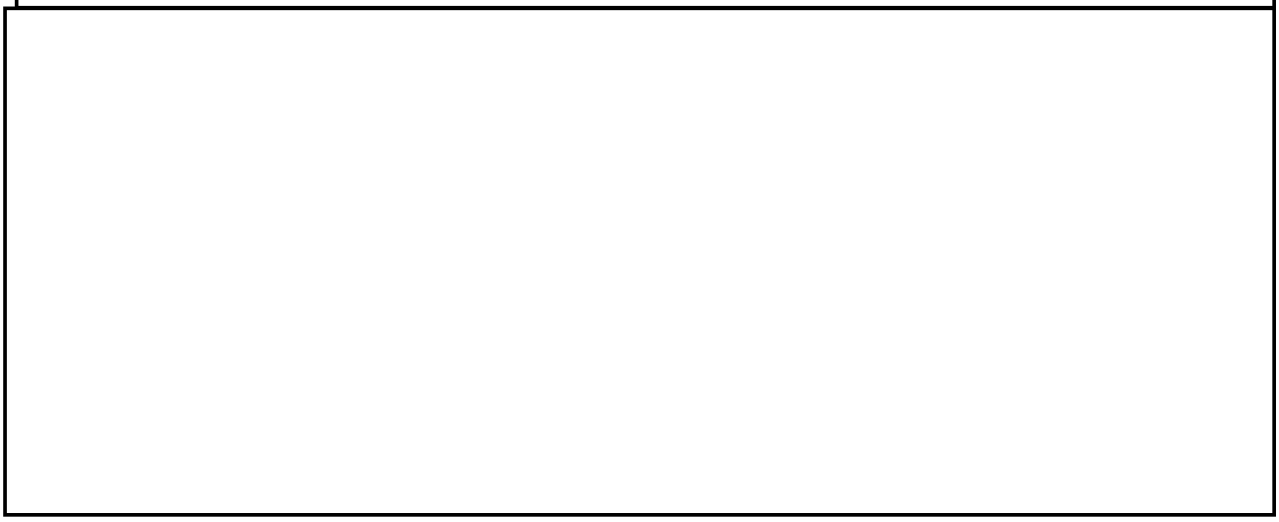
For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?



b5



b5

b5

b5

[redacted] b5

How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

[redacted] b5

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing.

[redacted] b5

possible. [redacted]

[redacted] In addition, as the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). For example, an effort is underway to prepare an MOU between DHS and DOJ regarding criteria and procedures for determining alien detainees of national security interest. In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other intitiatives, such as the Foreign Terrorist Tracking Task Force and the National Joint Terrorism Task Force have assisted in permitting better information flow with our law enforcement counterparts and will improve the handling of such cases. [redacted]

b5

82. OGC. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107- 56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeapor[dize] an investigation or unduly

[delay] a trial" been used? Please describe the circumstances in each of these cases?

b5

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response to Q84 b: The FBI disseminates intelligence information via Intelligence Information Reports (IIRs). With regard to 203 (b) material, the FBI does not track or keep a central database as to how many reports, if any, contain 203 (b) material.

b5

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

The FBI disseminates raw intelligence via the IIR. If 203 (b) material is disseminated it would be through this mechanism. The FBI does not keep a database as to whether 203 (b) material is contained with any disseminated IIR.

(1) If so, how many such reports have been issued?

Response: The FBI has no central database readily to determine the quantity of 203 (b) material disseminations through the aforementioned methods.

During the period August, 2002 (the beginning time-frame in which statistical data was collected), through August, 2004, the Counterterrorism Division has disseminated approximately 3860 IIRs. Of that total, 240 of those IIRs contain FISA-derived intelligence. The remaining number of IIRs are derived from various sources and methods which may or may not include Title 3

derived information. In addition, other divisions besides the Counterterrorism Division disseminate IIRs.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

[redacted] b5

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response: The FBI disseminates raw intelligence via the IIR. If 203 (d) material is disseminated it would be through this mechanism. The FBI does not keep a database as to whether 203 (d) material is contained in any disseminated IIR.

[redacted] b5

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

Response: Dissemination of Electronic, Wire, and Oral Interception Information to the IC derived through standard criminal procedures may be effected electronically through IIRs, TM, Intelligence Assessments, Intelligence Bulletins. However, dissemination of this intelligence information also may be transacted through the exchange of FBI Letterhead Memoranda (LHMs) among relevant IC members.

(1) If so, how many such reports have been issued?

Response: The FBI has no central database to determine the quantity of 203(d)material disseminations through the aforementioned methods.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

b5

[redacted] b5

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

[redacted] b5

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: [redacted] b5

OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information.

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication

facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

[redacted] b5

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. [redacted] b5

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community, [redacted] b5 **through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins.**

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence [redacted] b5 [redacted] Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners, [redacted] b5

In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, [redacted] access and responsiveness to local FBI field office, [redacted] b5

FBI program and national intelligence requirements . The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the

target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

[redacted] b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

(i) How many of such cases were terrorism-related?

b5

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation

disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

(S)

b1
b2
b7E

(S)

b5

(U)

b5

[redacted] b5

[redacted] b2 b7E b5

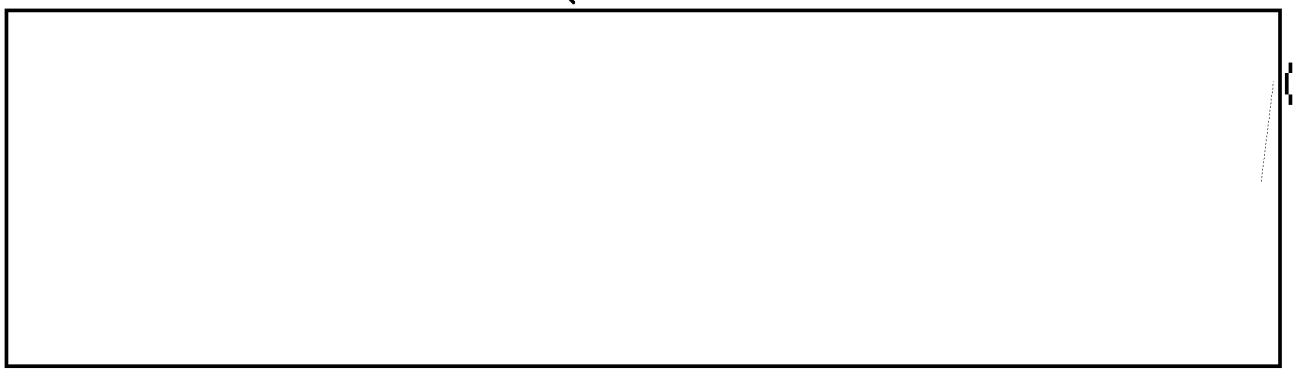
[redacted]. (U)

[redacted] b5

[redacted] (U)

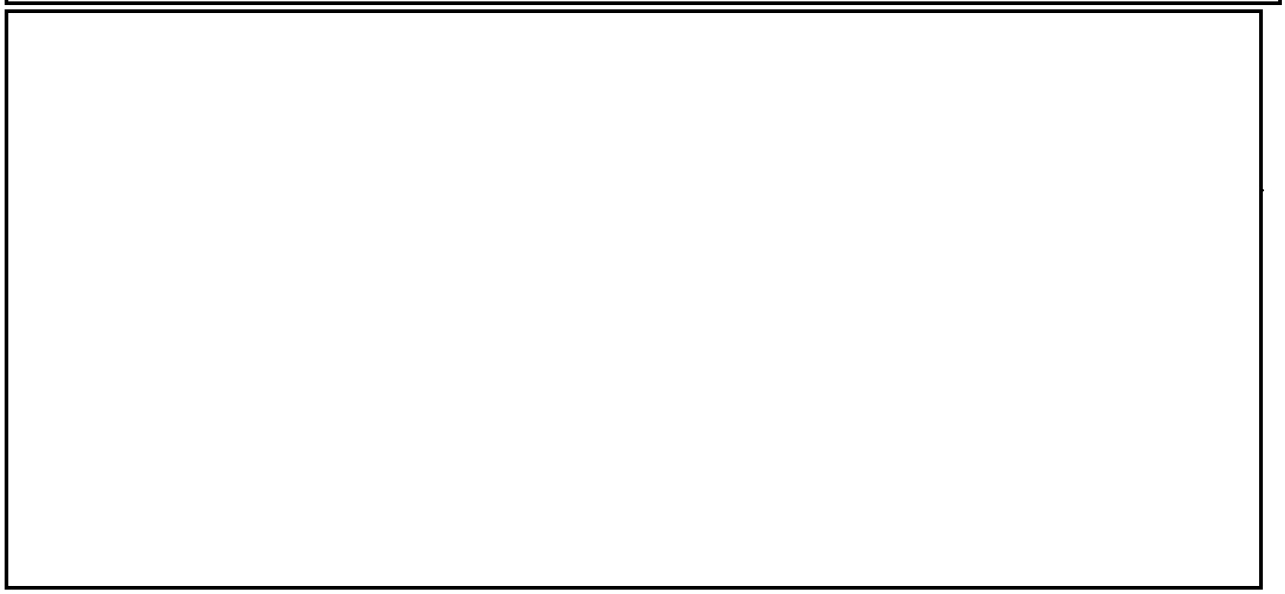
d. [redacted] b1 b2 b7E b5

[redacted] S)

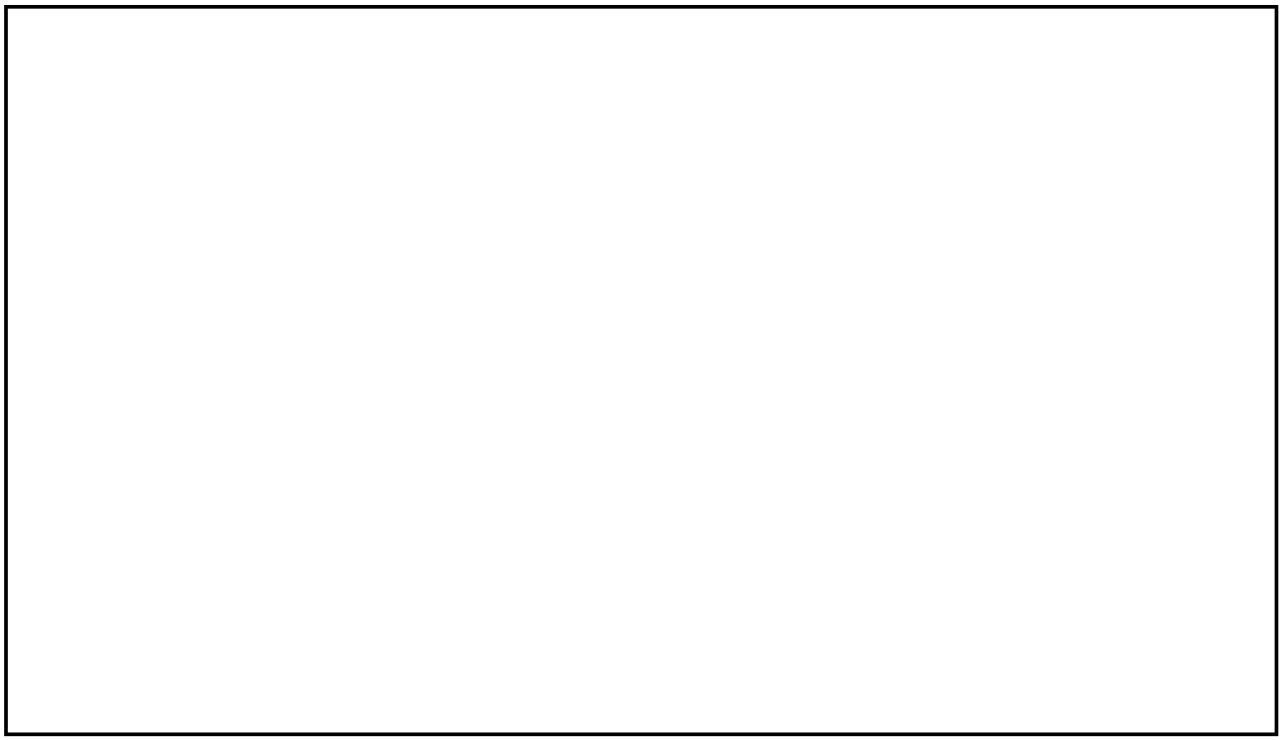


(S)

b1



b5



b5

[redacted]

[redacted] b5

[redacted] b5

[redacted]

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law

during the period since its passage, are there changes to this statute which the Congress should consider?

[redacted] b5

[redacted] b5

[redacted]

[redacted] (S)

(S) [redacted] b1 b5 b7A

[redacted]

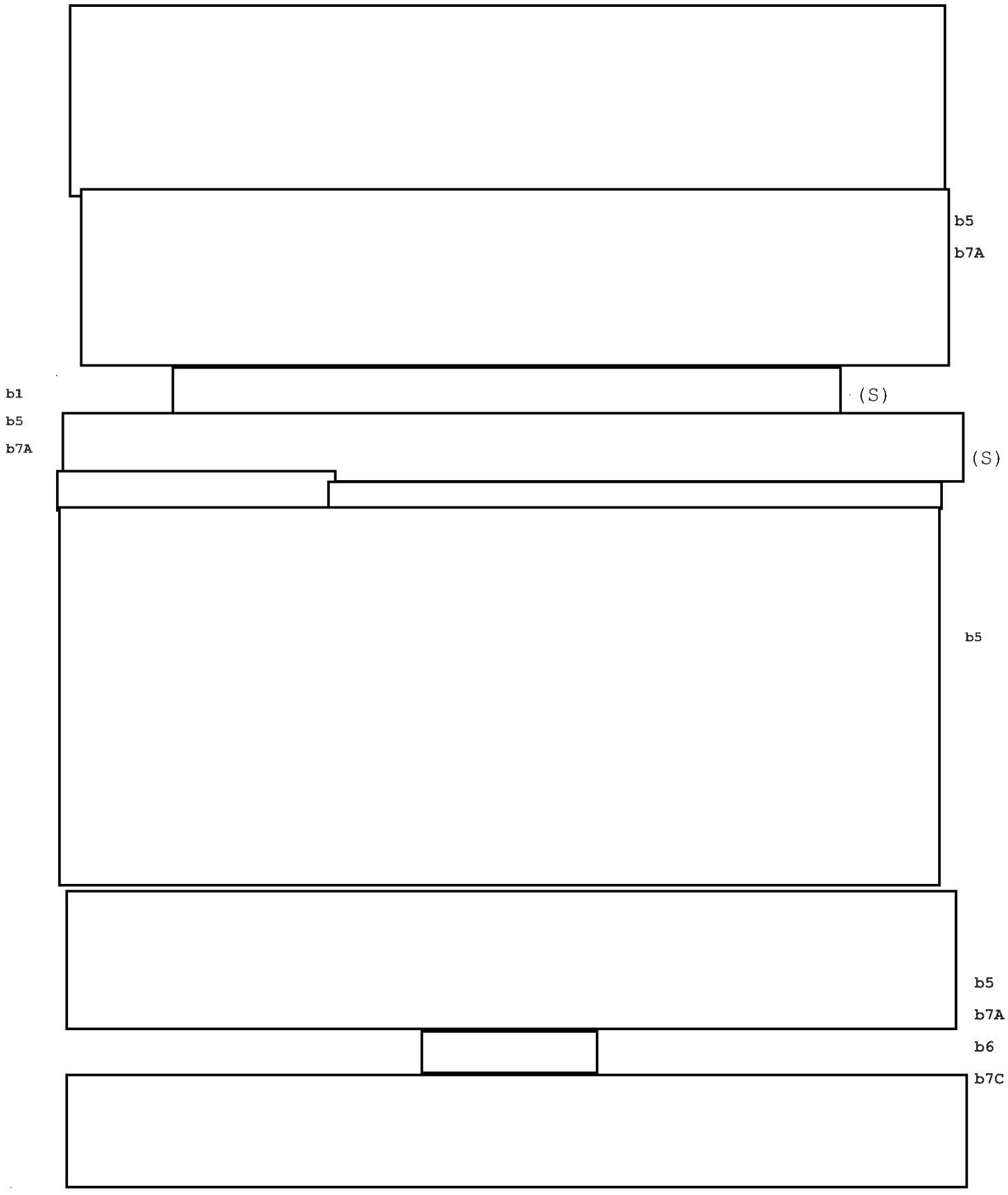
(S)

b1
b5
b7A

(S)

[redacted]

b5
b7A
b6
b7C


b5
b7A
b1
b5
b7A
(S)
(S)
b5
b5
b7A
b6
b7C

[redacted]

b5
b6
b7C

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

[redacted]

b5

101 d. OGC. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

[redacted]

b6
b7C
b5

100 e. CTD (in coordination with OGC). Mayfield has stated that he

believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.

b1
b5
b6
b7C

(S)

103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

(S)

b1
b5
b6
b7C

(S)

b. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any means appropriate to the circumstances, including Intelligence Information Reports (IIRs), Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(b) material?

Response:

The FBI disseminates intelligence information via the IIR, which is an electronic communication format widely accepted in the IC as the standard intelligence dissemination vehicle. IIRs consist of raw intelligence (intelligence which has not been finally evaluated) and associated clarifying information that puts the raw intelligence into context. IIRs are drafted and prepared by the FBI's cadre of Intelligence Analysts/Reports Officers. Before FBI intelligence is disseminated, it is analyzed and sanitized to protect intelligence sources and methods and, if applicable, United States persons and entities that may be compromised or negatively impacted if left unprotected. FBI Program Managers and Intelligence Analysts concurrently identify intelligence that is consistent with IC intelligence requirements and interests.

(1) If so, how many such reports have been issued?

Response:

Although CTD is not the only FBI producer of IIRs, that Division reports that, during the period from August 2002 (when statistical data was first collected) through August 2004, CTD has disseminated approximately 3,860 IIRs [redacted] The remaining IIRs have been

b2
b7E

derived from various sources and methods which may or may not include Title III information.

The FBI does not track or maintain a central database with respect to the number of IIRs containing 203(b) material, if any.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Determinations to disseminate electronic, wire, and oral intercept information are made with input from Operational Program Managers, Intelligence Analysts, the National Security Law Branch, and, when appropriate, DOJ. This evaluation considers the value of the information not only to the IC but also, depending on the proposed use, context, and nature of any threat-related information, to federal, state, and local law enforcement entities and, when authorized by DOJ, to foreign intelligence services and foreign law enforcement agencies.

The quality and value of IIRs are evaluated through several means. On each IIR, the Reports Officer provides information by which the customers can contact the Reports Officer directly. The quality and relevance of the reporting is also reflected by the submission of additional collection requirements; IC members often forward formal Requests for Information (RFIs) with respect to information that has been protected (not provided) in the IIR, such as U.S. Person information. Such RFIs provide an excellent indication of IC interest in FBI reporting. In addition, IC members often provide feedback with respect to specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. The FBI's OI also often receives evaluations of FBI reporting, and is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

c. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response:

The FBI shares foreign intelligence information, as defined in Section 203(d)(2), with the IC through several conduits. Dissemination can be through direct classified and unclassified IIRs, Intelligence Assessments, Intelligence Bulletins,

Teletype Memoranda, or IC web sites on classified networks. The FBI also shares intelligence information through the FBI's Joint Terrorism Task Forces (JTTFs), which include members of the IC and operate in 100 locations across the United States. Unclassified but "law enforcement sensitive" intelligence information is also disseminated to federal, state, and local law enforcement intelligence components through Law Enforcement Online (LEO), a computer network which provides finished intelligence products, assessments, and bulletins on significant developments and trends.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any appropriate means, including IIRs, Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(1) If so, how many such reports have been issued?

Response:

While the FBI does not track or maintain a central database with respect to the number of IIRs containing 203(d) material, if any, the July 2004 DOJ "Report From the Field: The USA PATRIOT Act at Work" indicates that DOJ has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, to track terrorists' funding sources, and to identify terrorist operatives overseas.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

There are various means by which IIRs are evaluated. Members of the IC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify the means by which customers can contact them directly. IC members assess the quality and relevance of the reporting, and submit additional collection requirements when appropriate. Often, IC members forward formal Requests for Information (RFIs), which can provide an excellent indication of IC interest in FBI reporting. The FBI's OI also receives evaluations of FBI reporting. The OI is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

d. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response:

Pursuant to Section 905, DOJ developed the Attorney General's Guidelines Regarding Information Sharing under the USA PATRIOT Act. These guidelines are available on the website of DOJ's Office of Legal Policy (OLP) (www.usdoj.gov/olp). Additionally, among other Department materials relating to information sharing are the following:

- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, Part VII.B. (10/31/03) (concerned in part with information sharing with intelligence agencies) – Portions of these guidelines are classified, but Part VII.B., relating to information sharing, is unclassified and appears without deletions on OLP's website.

- Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (3/4/03).

- Memorandum from the Attorney General entitled, "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation" (9/23/02) – Available on OLP's website.

- Memorandum from the Attorney General entitled, "Coordination of Information Relating to Terrorism" (4/11/02) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

- Memorandum from the Attorney General entitled, "Prevention of Acts Threatening Public Safety and National Security" (11/8/01) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

- Memorandum from the Attorney General entitled, "Disseminating Information to Enhance Public Safety and National Security" (Sept. 21, 2001) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

e. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the [redacted] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6
b7C

f. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

b5 [redacted]

85. Section[ ] 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains [to] the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. How often has this authority been used, and with what success?

Response:

The response to this question is classified and is, therefore, provided separately.

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response:

FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. The FBI shares many forms of foreign intelligence with other members of the IC through direct classified and unclassified disseminations, through web sites on classified IC networks, through its participation in Joint Terrorism Task Forces (JTTFs), and through its collaboration in activities abroad.

FBI intelligence products shared with the IC include IIRs, Intelligence Assessments, and Intelligence Bulletins. The FBI also disseminates intelligence information through LEO, a virtual private network that reaches federal, state, and local law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes available to all users finished FBI intelligence products, including intelligence assessments resulting from the analysis of criminal, cyber, and terrorism intelligence, finished intelligence concerning significant developments or trends, and IIRs that are available at the SBU level. In addition, the FBI recently posted the requirements document on LEO, providing to state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response:

In the past two years, CTD's Terrorism Reports and Requirements Section has disseminated 76 IIRS containing information derived from FISA-authorized surveillance and/or searches. (Statistics are not maintained in a way that would enable us to advise whether any of the FISA-derived information in the reports was obtained using roving wiretap authority.) Other FBI Divisions have also issued reports containing FISA-derived information. For example

b2
b7E

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

The OI promulgated the FBI's Intelligence Information Report Handbook on 7/9/04. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The OI is also working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with law enforcement and IC partners.

In addition, the FBI's Inspection Division has established criteria for assessing: the value of human source reporting; access to and the responsiveness of local FBI field offices; and FBI program and national intelligence requirements. The OI is developing guidelines for using these same criteria to assess the value of raw intelligence. Initial discussions on this issue have been held with the CI, CT, Criminal, and Cyber Divisions, and the results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response:

No, DOJ does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept

the conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, for surveillance of all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the FISA Court issue, along with the primary order, a "generic" secondary order with respect to a specifically identified FISA target that the FBI can serve in the future on a currently unknown cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear, in a detailed affidavit, to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. While the roving order carries the additional requirement of a judge's approval to monitor more than one telephone, it permits government agents to continue to monitor the target, even if the target changes to a different cellular telephone, rather than first going through the lengthy application process to monitor that new phone. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the FISA Court for a new secondary order. The FBI views this as a vital tool to follow targets who change cell phone providers or other communication channels as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response:

The FBI does not file briefs with the FISA Court. While OIPR files briefs with that Court on behalf of DOJ and the government, it has filed no such briefs on this subject.

d. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act? If so, please describe the nature and disposition of such a complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending [redacted] b6 b7C investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

Response:

We are not aware of any systematic reviews in this area, either by the FBI or DOJ.

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate?

Response:

None of which the FBI is aware.

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending [redacted] investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6
b7C

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

None at this time.

87. Section 209 of the USA-Patriot Act clarified the law with regarding the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. How many such search warrants have been issued since passage of this act?

Response:

The FBI does not collect or maintain statistics concerning the types of search warrants issued in FBI investigations, including those seeking access to voice mail. Because federal search warrants are requested by U.S. Attorneys' Offices and issued by U.S. District Courts, these statistics may be maintained by one or both of those offices.

b. In such cases, have there been any instances in which a wiretap, as opposed to a search[ ] warrant[,] would not have been supported by the facts asserted in support of the search warrant.

Response:

This information is unavailable, as indicated above. It is clear, however, that the support needed for a federal wiretap is considerably greater than that required for a search warrant.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

A private citizen who has lodged numerous complaints against the FBI, all of which have been determined to be unfounded pursuant to appropriate inquiry, complained that she was a former FBI employee whose home, vehicles, telephone, and internet had been subject to "aggressive surveillance" since August 2000. FBI investigation revealed that the complainant was, in fact, not a former FBI employee and that the FBI had conducted no surveillance of her for any reason. Based on these findings, this matter was closed by the FBI in July 2003. The FBI has construed this as a complaint with respect to both Section 209 and 217 of the USA PATRIOT Act.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI is not aware of any substantive changes to this provision warranting Congressional consideration. Section 209 is, however, currently scheduled to expire at the end of 2005, and the FBI strongly supports making this provision permanent. Section 209 allows investigators to use court-ordered search warrants to obtain voice-mail messages held by a third party provider when supported by probable cause. Previously, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. 2703, allowed law enforcement authorities to use search warrants to gain access to stored electronic communications such as e-mail, but not stored wire communications such as voice-mail. Instead, the wiretap statute, 18 U.S.C. 2110(1), governed access to stored wire communications, requiring law enforcement officers to use wiretap orders to gain access to unopened voice-mail. This resulted in voice-mail messages being treated differently than e-mail messages. Voice-mail messages are also treated differently than answering machine messages inside a home, access to which requires a search warrant, because answering machine messages are not regulated under the wiretap statute. Section 209 of the USA PATRIOT Act eliminates the disparate treatment of similar information. If this section is sunsetted, voice-mail messages will again be treated in a different manner than answering machine messages and stored e-mail information beginning in 2006.

88. Section 212 of the USA-Patriot Act permits communications service providers to provide customer records or the content of customer communications to the FBI in an emergency situation. This question pertains to application of this provision since its passage, and to all instances, not only to terrorism investigations.

a. In how many cases has this provision been used? Please provide a short description of each such case to the Committee.

Response:

Service providers have voluntarily provided information on at least 141 occasions under this provision. Such disclosures have often included both e-mail content and associated records. Several of these disclosures have directly supported terrorism cases under the emergency of a possible pending attack. For example, this provision has been used to obtain access to e-mail accounts used by terrorist groups to discuss various terrorist attacks. It has also been used to respond quickly to bomb and death threats, as well as in an investigation into a threat to a high ranking foreign official. This provision has additionally been used to locate kidnaping victims and to protect children in child exploitation cases. In one kidnaping case involving the abduction of a 14-year-old girl, reliance on this

provision allowed the FBI to quickly locate and rescue the child and to identify and arrest the perpetrator. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours.

b2
b7E

Because many international service providers are located within the United States (such as [redacted], Legal Attachés have used this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss of life or serious injury.

Additional examples are provided in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work."

b. In any such case have there been any cases in which, except for the time constraints imposed by the emergency situation, a conventional wiretap or search warrant, would not have been supported by the facts available to the Government at the time of the emergency request? If so, please describe such situations.

Response:

We are aware of no such circumstances. However, it is important to recognize that the information that may be disclosed under this emergency authority is limited to the contents of communications that are in electronic storage and records associated with customers or subscribers. Given this limitation, a conventional wiretap would generally not apply, and a search warrant would be required only for the contents of communications in 'electronic storage' (e.g., incoming email not yet retrieved by the subscriber) less than 181 days old. Emergency authority is appropriate for the disclosure of information held by a third party and, to the extent the information is constitutionally protected, disclosure of the information under exigent circumstances is entirely consistent with the emergency exception to the warrant requirement of the Fourth Amendment.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the [redacted] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section. b6 b7C

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

There is currently a discrepancy between the emergency provisions applicable to contents and records that appears illogical and unjustified. Currently a provider is arguably required under 18 U.S.C. 2702(c)(4) to meet a higher burden for disclosing a record or other subscriber information than is required by § 2702(b)(7) for divulging the contents of a communication in electronic storage. Moreover, the entities to whom a provider may disclose are significantly more restricted for records than for content. The language in (b)(7) was enacted by Pub. L. 107-296 as part of the Homeland Security Act of 2002, with the objective that all entities with responsibility for ensuring our domestic security would have access to this information in an emergency. It does not appear that the discrepancies between the disclosure of content and records are supported by differing privacy interests inherent in the respective information or by other factors. Accordingly, reconciling these provisions would be appropriate.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. In how many cases has this authority been used?

(i) How many of such cases were terrorism-related?

Response to a and a(i):

The FBI does not maintain this information. It is, instead, maintained by DOJ's OIPR, to whom the FBI defers for response.

b. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response:

[redacted] b5

c. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.

Response:

The FBI has not developed any such regulations or directives, nor is it aware that the IC or DOJ have issued guidance defining "non-content communications" in relation to the use of FISA pen register/trap and trace authorities.

d. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

See response to Question 85b, above.

(i) If so, how many such reports have been issued?

Response:

See response to Question 85b(i), above.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

See response to Question 85b(ii), above.

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

Response:

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be conducted solely on the basis of activities protected by the First Amendment.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA).

b2
b7E

When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

The only instance when the Department has declassified the number of times section 215 has been used was on 9/18/03 – not in October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated 12/23/04.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, however, terrorists and spies have used libraries to plan and carry out activities that threaten our national security, and it is important that we not permit these facilities to become safe havens for terrorist or other illegal activities. The PATRIOT Act permits those conducting national security investigations to obtain business records – whether from a library or any other business – with the permission of a federal judge.

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence

activities conducted by the IC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

[redacted] b5

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Although the FBI has procedures to evaluate the quality of intelligence reports, no reports have been disseminated which contained information acquired pursuant to section 215 of the USA PATRIOT Act.

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

b6
b7C

The OIG has advised that, with the possible exception of the pending [redacted] investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

91. Section 217 of the USA-Patriot Act authorizes, without court order, the interception of communications to and from a trespasser with a protected computer. This question pertains to the implementation of this provision since its passage.

a. How many times has the authority under this section been used, and with what success? Please provide descriptions of the circumstances where it has been used.

Response:

While the FBI does not maintain statistics on the frequency with which the trespasser authority has been used, we can provide examples of some such cases.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). This group used chat rooms and fraudulent web sites, creating false identities to obtain e-mail accounts and then transmitting their communications through a computer that had been "hacked" and set up to operate as their proxy server. A proxy server changes an Internet user's original Internet protocol (IP) address to that of the proxy server so that only the proxy server knows the true point of origin. The owner of the hacked computer was not aware that it was being used as a proxy server, and considered all individuals using the system as a proxy server to be trespassers. The owner provided the FBI with consent to monitor the communication ports solely used by the trespassers, and this monitoring led to the subject's true identity. The subject was indicted in September 2003. Without this authority to monitor, the real identities of the trespassers could easily have remained anonymous.

In another example, a former employee was suspected of illegally accessing a company's e-mail system to gain inside information regarding company concepts and client information, as well as privileged information regarding legal proceedings between the company and the former employee. The computer intruder used a variety of means to access the system, including wireless modems in laptops and hand-held Blackberry devices, making it more difficult to identify the intruder and to link the computer intrusions to the former employee. The victim company authorized the FBI to monitor the intruder's communications with and through its computer systems.

In another case, a computer-intruder obtained control of a school's network and reconfigured it to establish additional IP addresses that were separate and distinct from those used by the school. This allowed hackers, and others using the Internet who did not want to be located, to jump through the school's system before committing their illegal acts. Monitoring accomplished pursuant to the school's consent resulted in the FBI's identification of over 200,000 different IP addresses using the school system as a proxy to further illegal activity such as fraud, computer intrusions, and spamming.

As these cases make clear, this authority is critical not only to the FBI's ability to identify criminals who engage in computer intrusions but also its ability to

identify and investigate additional criminal activities conducted through victims' computers.

b. Section 217(2)(I) requires authorization by the owner of the computer before the section can be applied. Can this authorization be withdrawn or limited by the owner of the computer? If so, how and in what circumstances?

Response:

Yes. As with any form of consent, which must be freely and voluntarily given to be valid, the consenting party has the right to terminate the consent at any time. The FBI encourages the use of a written consent form containing an express acknowledgment by the consenting owner or operator that states: "I understand my right to refuse authorization for interception and have accordingly given this authorization freely and voluntarily."

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

See response to Question 87c, above.

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

Response:

As indicated in the July 2004 DOJ publication entitled, "Report from the Field: The USA PATRIOT Act at Work," the removal of the "wall" played a crucial role in the Department's successful dismantling of a Portland, Oregon, terror cell, popularly known as the "Portland Seven." Members of this terror cell had

attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned through an undercover informant that [redacted] While several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them. Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest [redacted] immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack; if prosecutors had arrested [redacted] in order to prevent a potential attack, the other suspects in the investigation would undoubtedly have scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, FBI agents could conduct FISA surveillance of [redacted] to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets, and could keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest [redacted] prematurely, but instead to continue to gather evidence on the other cell members. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops on 10/3/03.

b6
b7C
b7D

DOJ shared information pursuant to sections 218 and 504 before indicting [redacted] and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist organizations, responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that [redacted] served as the secretary of the PIJ's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ. Sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against [redacted] and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to prosecutors' ability to build their case and pursue the proper charges.

b6
b7C

Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the so-called "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, some of whom trained for jihad in Northern Virginia by participating in paintball and paramilitary training or traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against several individuals. Nine of these defendants have received sentences ranging from four years to life imprisonment (six of these sentences were pursuant to guilty pleas and three were contrary to their pleas; charges have included conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban).

Information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was also pivotal in the investigation of two Yemeni citizens [redacted] and [redacted] who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. [redacted] the complaint alleges that [redacted] had boasted that he had personally handed Usama Bin Laden $20 million from his terrorist fund-raising network and that [redacted] had flown from Yemen to Frankfurt, Germany, in 2003 with the intent to obtain $2 million from a terrorist sympathizer [redacted] who wanted to fund al Qaeda and HAMAS. During their meetings, [redacted] were extradited to the United States from Germany in November 2003 and are currently awaiting trial.

b6
b7C
b7D

Sections 218 and 504 were also used to gain access to intelligence that facilitated the indictment of [redacted] Benevolence International Foundation (BIF). [redacted] conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. [redacted] had a long-standing relationship with Usama Bin Laden, and used his charities both to obtain funds for terrorist organizations from unsuspecting Americans and to serve as a channel for people to contribute money knowingly to such groups. [redacted] pled guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

b6
b7C

The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the San Diego prosecution of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they had conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they had conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

Sections 218 and 504 were also critical in the successful prosecution of [redacted] who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq and of two counts of perjury. Before the Gulf War [redacted] passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of [redacted] pursuant to FISA shared information with law enforcement agents and prosecutors investigating [redacted] Through this coordination, law enforcement agents and prosecutors learned from intelligence officers that [redacted] was acting as an agent of the Iraqi government, providing a compelling piece of evidence at [redacted] trial.

b6
b7C

b. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

b6
b7C

The OIG has advised that, with the possible exception of the [redacted] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA

PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FISA Court of Review has made clear that the "significant purpose" standard is constitutional. Accordingly, additional changes are unnecessary.

93. Section 220 of the USA-Patriot Act, "Nationwide Service of Search Warrants for Electronic Evidence" allows for the execution of a search warrant seeking electronic data anywhere in the country. This question pertains to the implementation of this provision since its passage.

a. In how many cases has this authority been used?

Response:

While the FBI does not require or maintain centralized statistics on the use of search warrants, Field Offices indicate that they have routinely relied on this provision (codified at 18 U.S.C. 2703(a)) and can safely estimate that, nationwide, this search authority has been used at least 100 times since its passage.

In section 220 of the USA PATRIOT Act, Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The ability to obtain this information with greater efficiency has proven invaluable in numerous cases, including: several terrorism investigations (such as the Virginia Jihad case described above and a complex terrorism financing case in which it was used to obtain a subject's e-mail related to a 7/4/02 shooting at Los Angeles International Airport); child pornography cases in which it is used to obtain information from ISPs regarding those trading sexually exploitive images of children; investigations of "carders" (those who use and trade stolen credit card information); and numerous investigations into Internet sales of counterfeit products, which have led to several indictments and the seizure of bank and financial accounts.

Child pornography cases highlight the benefit of Section 220, because the ability to obtain a search warrant in the jurisdiction of a child pornography investigation rather than in the jurisdiction of the ISP is critical to the success of a complex, multi-jurisdictional child pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country so they could obtain warrants in those jurisdictions, or travel hundreds or thousands of miles to present warrant applications to local magistrate judges. Without Section 220, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

The following case, included in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work," provides an additional example of the benefits afforded by Section 220. A man, armed with a sawed-off shotgun, abducted his estranged wife and sexually assaulted her. Then, after releasing his wife, he fled West Virginia in a stolen car to avoid capture. While in flight, he contacted cooperating individuals by e- mail using an Internet service provider (ISP) located in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, including the California ISP. Within a day of the order's issuance, the ISP released information revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and noticed a carnival set up next to the public library. Because they were aware that the fugitive had previously worked as a carnival worker, the Deputy Marshals went to the carnival and discovered the stolen car, arresting the fugitive as he approached the car. He later pled guilty in state court and was sentenced to imprisonment for 30 years. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account, made possible by section 220 of the USA PATRIOT Act, was crucial to his capture.

Section 220 has also made the process of obtaining a warrant for ISP information much more efficient. Before the USA PATRIOT Act, judicial districts that are home to large ISPs were inundated with search warrant requests for electronic evidence. For example, the U.S. Attorney's Office in Alexandria, Virginia, was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for the records of an ISP located there. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all the details of another district's investigation in order to present an affidavit to the court in support of the search warrant application. Because of section 220, however, these attorneys and Agents can now spend their time on local cases and investigations rather than on learning the details of unrelated investigations being worked

through distant offices. Given the short time for which ISPs typically retain records, this provision has enabled the FBI to obtain critical information that may otherwise have been lost or destroyed in the ordinary course of the ISP's business. Section 220 also results in a more efficient use of judicial resources by allowing the judge with jurisdiction over the offense to issue the warrant and retain oversight over the search.

b. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the [redacted] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section. b6 b7C

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

94. Section 223 of the USA-Patriot Act creates a cause of action for willful violations of Title III's electronic surveillance procedures. Have any such lawsuits been brought? If so, please provide details of each such case.

Response:

No such lawsuits have been brought.

95. Section 225 of the USA-Patriot Act provides immunity for those who aid in the execution of a FISA order. Has such immunity been invoked? If so, please describe any such case.

Response:

No. Immunity has not been claimed under this section with respect to FBI investigations in either the civil or criminal context.

96. The following question pertains to surveillance conducted pursuant to the FISA.

a. What is the backlog on processing of intercepts? What is the average time between interception and first monitoring.

b. What percentage of intercepts that are not in English are translated within 24 hours? A week?

c. How many hours of FISA intercepts remain untranslated as of May 20, 2004?

Response to a through c:

FBI Director Mueller has made clear his interest in having all material derived from the FBI's use of FISA authority reviewed and analyzed as quickly as possible. Since the majority of this material is in languages other than English, FBI Language Services Section personnel meet with the FBI's National FISA Manager and other management officials every two weeks to discuss national operational priorities and the most effective utilization of finite linguist resources. The operational plan established by this meeting is modified almost daily based on ever-shifting investigative priorities. These tactics ensure that all of the highest priority intelligence collected in a foreign language is reviewed immediately and that any outstanding work is limited to matters assigned a lower relative priority.

The FBI currently has sufficient translation capacity to promptly address all translation needs with respect to its highest priority, CT operations, often within 12 hours. While there are instances in which the FBI is not able to address translation needs as quickly as it would like, such as when the language or dialect involved is initially unidentifiable, this usually pertains to lower priority matters.

Conventional digital systems used to collect FISA-derived materials were not designed to measure the average time between intercept and initial monitoring. Recognizing the tactical value of having such aging reports for command and control purposes, a nationally integrated FISA statistical collection and reporting system has been developed and is undergoing a test and evaluation process to validate the mapping of meta data. This system should be fully functional by the end of calendar year 2004. It is clear, however, based on information provided by FBI field office managers, that the vast majority of communications in a foreign language relating to terrorism operations are being afforded full review by a qualified linguist within, at most, a few days of collection.

d. Please describe the process of indexing and retrieving FISA material.

Response:

Intelligence summaries from FISA intercepts are indexed and archived according to strict electronic surveillance (ELSUR) rules that make these summaries part of the official FBI record and allow these records to be searched in the Field Offices where the cases reside. Although recent progress has been made in creating an electronic archive of CI material that can be searched by authorized users fieldwide, CT summaries from FISA audio intercepts are not searchable in a central database at this time. The phased deployment of the ELSUR Data Management System (EDMS), starting in FY 2005, will make all intelligence summaries from FISA intercepts available in a searchable archive.

e. In the past 5 years, has there been a review or audit of the accuracy of FBI translations of intercepted or seized foreign language material?

Response:

Historically, translation reviews were normally conducted by field office managers on a semi-annual basis in conjunction with a linguist's performance appraisal rating. In order to standardize this procedure, the FBI's Language Services Section implemented minimum quality control standards and guidelines and assumed central management of the language services quality control program in January 2003. Quality control program guidelines stipulate which linguists' translations must be reviewed and at what intervals. The guidelines also identify those materials that must always be reviewed prior to dissemination.

Questions Posed by Senator Feingold

FBI Role in Iraq

97. a. How many special agents, translators, and other FBI employees have been assigned to work in Iraq since March 2003 and how many are currently there?

Response:

The response to this question is classified and is, therefore, provided separately.

b. Where were these agents, translators, and other employees assigned before they were sent to Iraq?

Response:

They were assigned to many of the FBI's offices, both in the field and at FBIHQ.

c. How many of these agents, translators, and other employees were working in the United States on terrorism cases?

Response:

15 percent of the FBI employees sent to Iraq were working on terrorism cases prior to that deployment.

FBI DNA Lab

98. The U.S. Department of Justice and Jacqueline Blake, a former biologist at the FBI DNA laboratory, recently entered into a plea agreement. Blake pled guilty to authoring and submitting over 100 reports containing false statements regarding DNA analysis she performed during a 2-1/2 year period from 1999 to 2002.

a. According to a Justice Department press release, the FBI has retested evidence in many of Blake's cases and has concluded that her false statements did not affect the outcome of any of the criminal cases in which she was involved. I assume that the FBI has notified the prosecutors in those cases. Has the FBI notified the courts and defense attorneys in each case in which Blake's falsified reports were involved? If not, why not?

sufficient to justify the delay. In addition, notice is only delayed; it is never eliminated. The searched party will, therefore, have the opportunity to challenge the validity and sufficiency of the reasons for delay and, if those reasons prove to be insufficient, to seek an appropriate remedy.

d. How many of the delayed notice warrants were issued with a (I) seven-day or less delay; (ii) 8 to 30 day delay; (iii) 31 to 60 day delay; and (iv) time period of 61 days or more and what were those time periods?

e. How many of the delayed notification warrants issued since the PATRIOT Act was passed were used in non-terrorism criminal matters?

f. Please provide the case name, docket number, and court of jurisdiction for each case in which a delayed notice warrant was issued since enactment of the PATRIOT Act.

Response to d through f:

This information was not collected in the EOUSA survey and is not otherwise available except through individual U.S. Attorney's Offices.

103. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

Response:

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

104. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518(11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

Response:

The requirements of the SAFE Act are inconsistent with, and more restrictive than, the requirements applicable to roving wiretaps in criminal investigations. In criminal cases, roving wiretap orders are limited to "such time as it is reasonable to presume that the [target] is or was reasonably proximate" to the facility. 18 U.S.C. 2518(11)(b)(iv). This does not require a conclusive determination that the target is actually present at the time of interception, as the SAFE Act would require, but only a reasonable belief under the circumstances that the facility or place is being used by the target. An analogous requirement is already contained in the Foreign Intelligence Surveillance Act (FISA). Under FISA, the FBI must demonstrate probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. 1805(a)(3)(B). In addition to these safeguards, both Title III and FISA require the use of procedures

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

Response:

By letter of December 23, 2004, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period January 1, 2004 through June 31, 2004.

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated December 23, 2004, and covered the period January 1, 2004 through June 31, 2004. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized

investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be premised solely upon the exercise of First Amendment-protected activities.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA). [redacted] b2 b7E [redacted] When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

The only instance when the Department has declassified the number of times section 215 has been used was on September 18, 2003 – not October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated December 23, 2004.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, terrorists and spies have used libraries to plan and carry out activities that threaten our national security. If terrorists or spies use libraries, we should not allow them to become safe havens for their terrorist or clandestine activities. The PATRIOT Act ensures that business records – whether from a library or any other business – can be obtained in national security investigations with the permission of a federal judge.

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence activities conducted by the USIC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

b5

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by employees of the Department of Justice. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of one matter, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response to a and b:

The responses to these questions are classified and are, therefore, provided separately.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be premised solely upon the exercise of constitutionally protected activities.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA). [redacted] b2 b7E

[redacted] b2 b7E When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

The response to this question is classified and is, therefore, provided separately.

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence activities conducted by the USIC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or

in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

b5

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

Response:

FBI (S)

DOJ By letter of December 23, 2004, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period January 1, 2004 through June 31, 2004. b1 b2 b7E

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response: b1

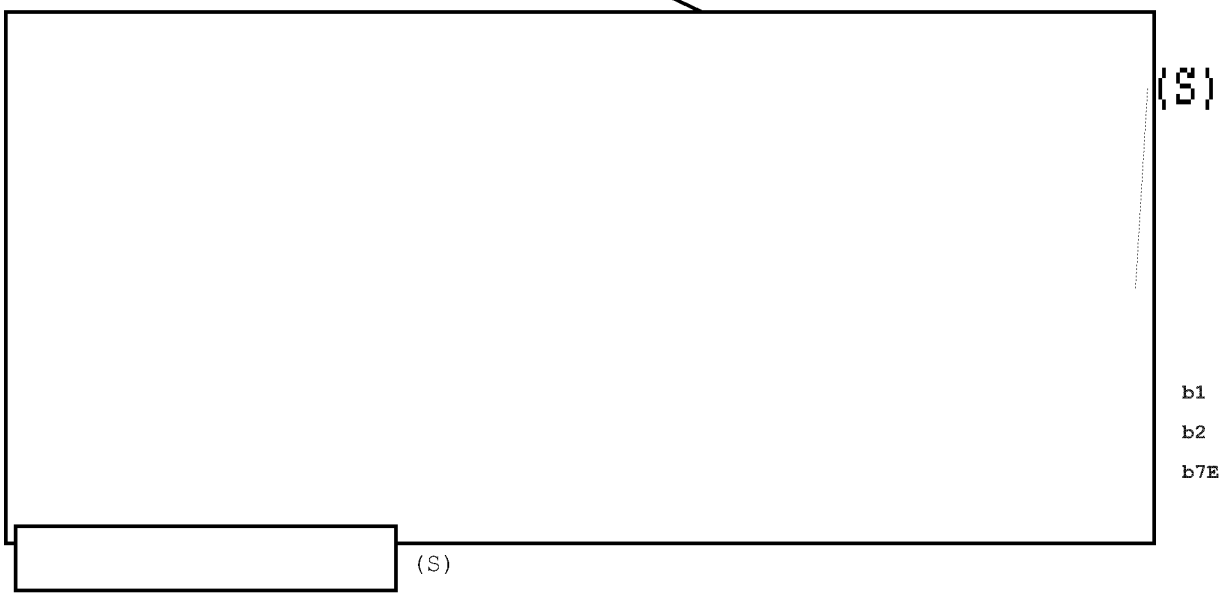
FBI (S)

DOJ The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated December 23, 2004, and covered the period January 1, 2004 through June 31, 2004. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

FBI (S) (S)
b1



DOJ The only instance when the Department has declassified the number of times section 215 has been used was on September 18, 2003 – not October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated December 23, 2004.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, terrorists and spies have used libraries to plan and carry out activities that threaten our national security. If terrorists or spies use libraries, we should not allow them to become safe havens for their terrorist or clandestine activities. The PATRIOT Act ensures that business records – whether from a library or any other business – can be obtained in national security investigations with the permission of a federal judge.

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

FBI The FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

DOJ

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by employees of the Department of Justice. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of one matter, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

MessageFrom: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 2:55 PM
To: [redacted] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b6
b7C

call it a day
-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Tuesday, September 14, 2004 2:43 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5

[redacted]

b2
b6
b7C

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 2:41 PM
To: [redacted] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

-----Original Message-----
From: [redacted] OCA) (FBI)
Sent: Tuesday, September 14, 2004 2:11 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED b6
NON-RECORD b7C

Toni:

[redacted] b5

[redacted]
Office of Congressional Affairs
JEH Building Room 7252 b6
[redacted] b7C
-----Original Message----- b2
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 1:43 PM
To: [redacted] OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED

b5

NON-RECORD

[redacted]

-----Original Message-----
From [redacted] (OCA) (FBI)
Sent: Tuesday, September 14, 2004 12:30 PM b6
To: FOGLE, TONI M. (INSD) (FBI) b7C
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

[redacted]
Office of Congressional Affairs
JEH Building Room 7252 b6
[redacted] b7C

-----Original Message----- b2
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 11:58 AM
To: [redacted] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

-----Original Message-----
From [redacted] OCA) (FBI) b6
Sent: Friday, September 10, 2004 4:07 PM b7C
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

[redacted] b2
Office of Congressional Affairs b6
JEH Building Room 7252 b7C
[redacted]

-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Friday, September 10, 2004 3:55 PM
To: [redacted] OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C b5

-----Original Message-----
From [redacted] (OCA) (FBI) b6
Sent: Friday, September 10, 2004 8:21 AM b7C
To: FOGLE, TONI M. (INSD) (FBI)
Subject: FW: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C b5

Thanks!

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

-----Original Message-----
From: THOMPSON, DONALD W. JR (RH) (FBI)
Sent: Thursday, September 09, 2004 6:26 PM b6
To: [redacted] (OCA) (FBI) b7C
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] I concur with the below responses. Thanks. DWT

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Thursday, September 09, 2004 5:54 PM
To: THOMPSON, DONALD W. JR (RH) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted]

b5

b6
b7C
b5

Thanks.

b2
b6
b7C

-[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

-----Original Message-----
From: THOMPSON, DONALD W. JR (RH) (FBI)
Sent: Thursday, September 09, 2004 5:42 PM
To[redacted](OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

-----Original Message-----
From [redacted] OCA) (FBI) b6 b7C
Sent: Thursday, September 09, 2004 2:13 PM
To: FOGLE, TONI M. (INSD) (FBI)
Cc [redacted] (INSD) (FBI); THOMPSON, DONALD W. JR (RH) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5

A/AD Thompson:

[redacted]

Thanks.

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Thursday, September 09, 2004 2:11 PM b2
To [redacted] (OCA) (FBI) b6
Cc [redacted] (INSD) (FBI); THOMPS b7C , DONALD W. JR (RH) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted]

Could you work out the language with A/AD Thompson this afternoon (I'm in a meeting that may take some time) -- leaving open this one situation? I'll ask [redacted] to work on the

questions you've asked on this open situation. T>

-----Original Message-----
From [redacted] (OCA) (FBI)
Sent: Thursday, September 09, 2004 2:04 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C
b5

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

-----Original Message-----
From [redacted] (INSD) (FBI)
Sent: Thursday, September 09, 2004 1:52 PM
To: [redacted] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

What do you think? b6
b7C
-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Thursday, September 09, 2004 8:46 AM
To: FOGLE, TONI M. (INSD) (FBI); THOMPSON, DONALD W. JR (RH) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

[redacted]
Office of Congressional Affairs
JEH Building Room 7252 b2
[redacted] b6
b7C
-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Thursday, September 09, 2004 8:42 AM
To: THOMPSON, DONALD W. JR (RH) (FBI); Hayn, Linda Susan (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] -- can we adjust the language accordingly?
-----Original Message-----
From: THOMPSON, DONALD W. JR (RH) (FBI)
Sent: Wednesday, September 08, 2004 6:01 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b5

-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Wednesday, September 08, 2004 1:08 PM
To: THOMPSON, DONALD W. JR (RH) (FBI)
Subject: FW: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted]

b5

b6
-----Original Message-----
From: [redacted] (OCA) (FBI)
b7C
Sent: Wednesday, September 08, 2004 12:40 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

Toni:

[redacted]

b6
b7C
b5

Thanks.

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Friday, September 03, 2004 9:42 AM
To: [redacted]OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5

[redacted]

-----Original Message-----
From: [redacted]OCA) (FBI)
Sent: Friday, September 03, 2004 9:00 AM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

Toni: b5

[redacted]

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

-----Original Message----- b2
From: FOGLE, TONI M. (INSD) (FBI) b6
Sent: Monday, August 30, 2004 12:45 PM b7C
To [redacted] (OCA) (FBI)
Cc [redacted] (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Friday, August 27, 2004 12:29 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: Complaints Re: FBI Implementation of Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

Toni:

[redacted] b5

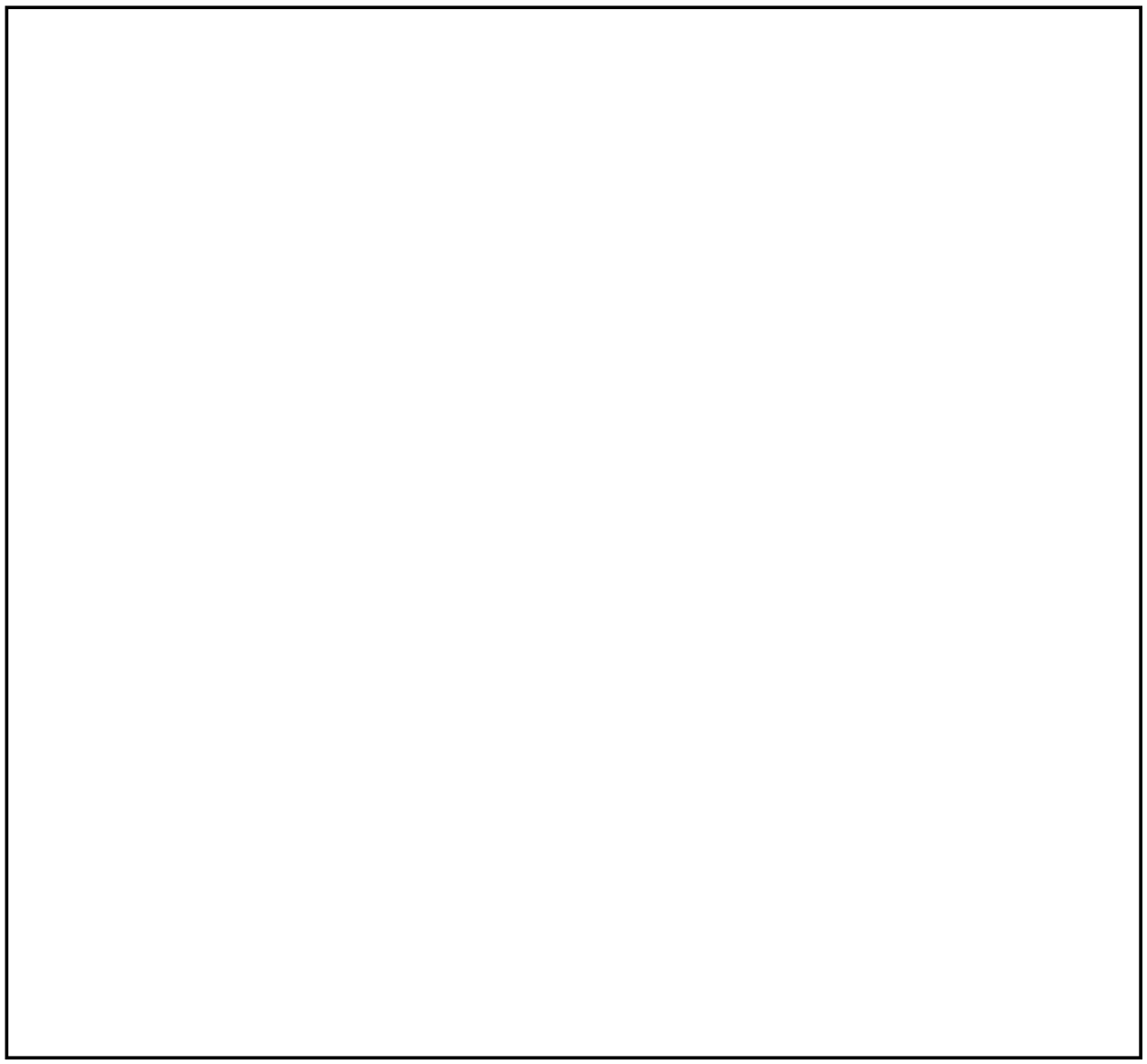
[redacted] b2
b6
b7C
b5

[redacted]

Office of Congressional Affairs
JEH Building Room 7252

[redacted]

[redacted] b5



b5

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-23-2005 BY 60309autam/mlt/lr2

MessageFrom: FOGLE, TONI M. (INSD) (FBI)
Sent: Friday, September 03, 2004 9:42 AM
To: [redacted](OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5
b6
b7C

[redacted]

-----Original Message-----
From [redacted](OCA) (FBI)
Sent: Friday, September 03, 2004 9:00 AM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

Toni:

[redacted]

b5

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Monday, August 30, 2004 12:45 PM
To [redacted](OCA) (FBI)
Cc [redacted](INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[redacted] b5

-----Original Message-----
From: [redacted] (OCA) (FBI) b6
Sent: Friday, August 27, 2004 12:29 PM b7C
To: FOGLE, TONI M. (INSD) (FBI)
Subject: Complaints Re: FBI Implementation of Patriot Act

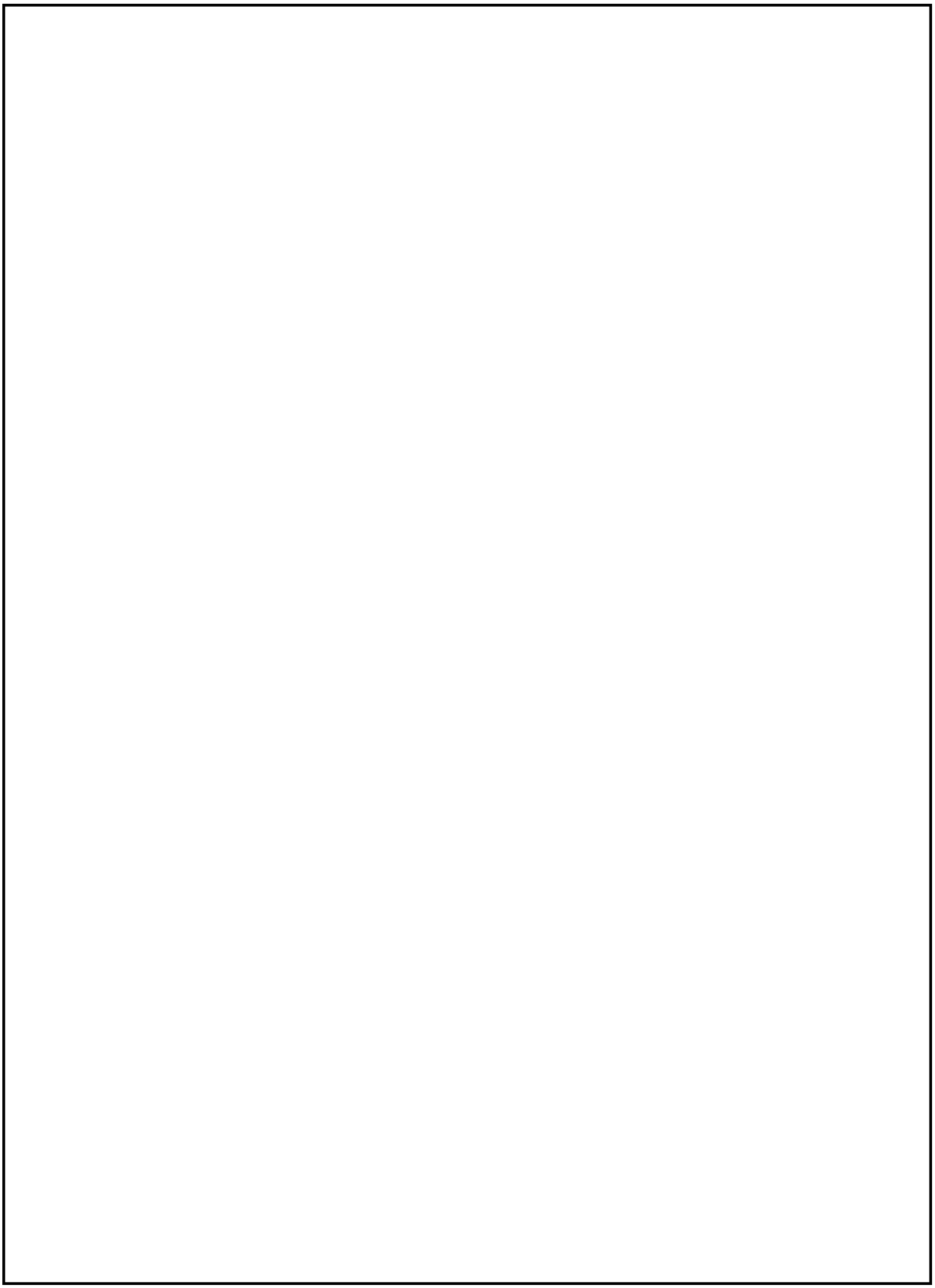
UNCLASSIFIED
NON-RECORD

Toni:

[redacted] b5

[redacted]

[redacted] b2
Office of Congressional Affairs b6
JEH Building Room 7252 b7C
[redacted] b5



b5

Questions for Investigative Law Unit

8. Office of the General Counsel (OGC). At the hearing on May 20, you stated that the Department of Defense had not, to date, referred any prisoner abuse cases involving military contractors to DOJ. The next day, DOJ announced that it had received such a referral the day before and that it had "opened an investigation into the matter."

a. At what time on May 20 did DOJ receive the referral from DOD?

Response:

b. When did you first learn about that referral?

Response:

c. Is the FBI conducting this investigation and, if not, what investigating body is?

Response:

b5

9. OGC. At the hearing, you noted that the CIA had referred a prisoner abuse case to DOJ, but that the investigation was being conducted by the CIA Inspector General and not the FBI. Has the FBI become involved in that investigation since the hearing? If not, what investigating body or bodies are involved?

Response:

56. Has a final decision been made as to whether prior approval is mandatory for visiting a public place or attending a public event to detect or prevent terrorist activity?

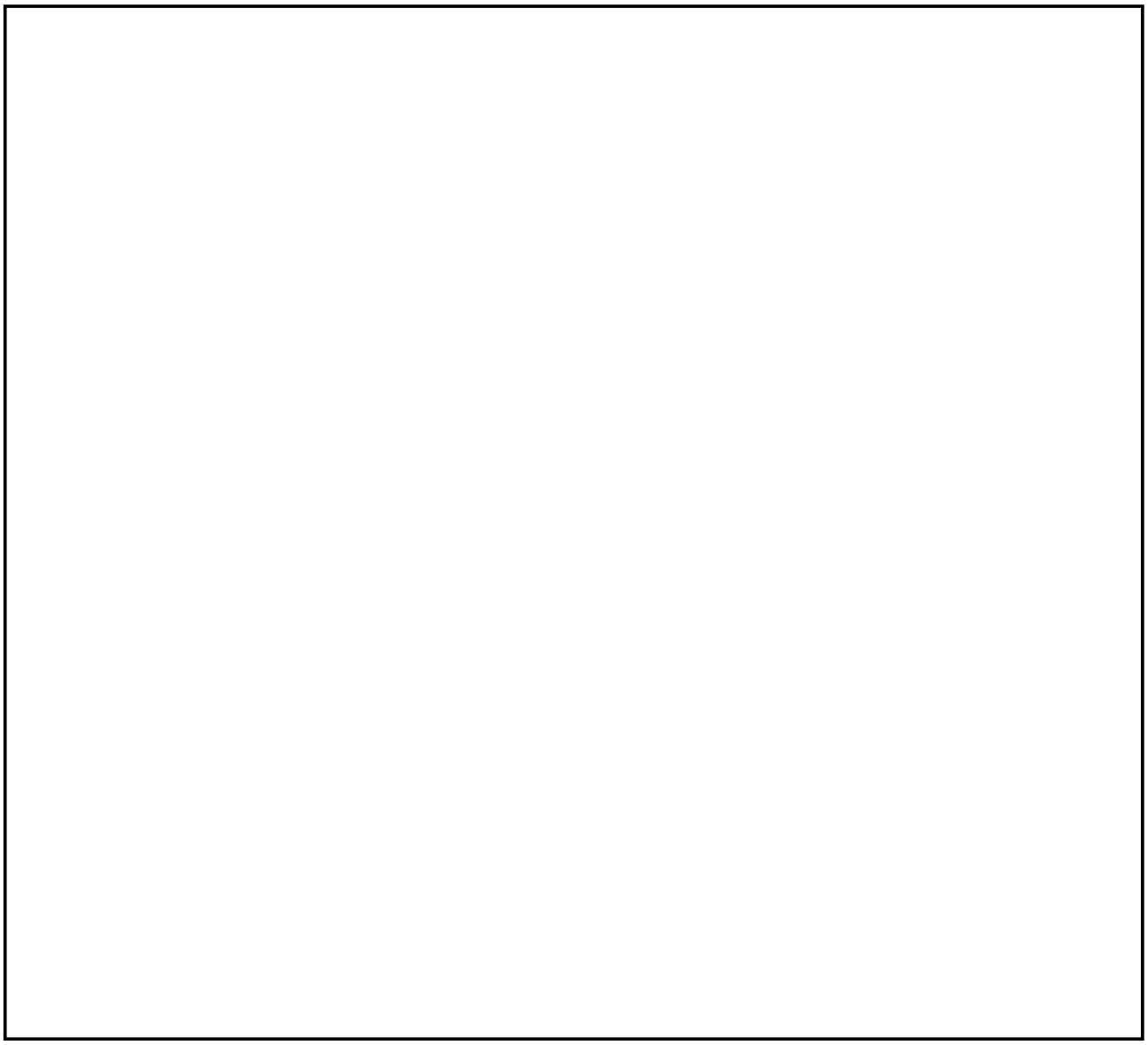
Response:

[redacted]

b5

66. Has the FBI implemented any new professional rules of conduct or code of ethics policies that provide safeguards against FBI abuse of its PATRIOT Act authorities? What, if any, internal or disciplinary punishments are in place for abuses by employees?

Response: [redacted]



b5

80. The authority to arrest and detain a person whose "testimony . . . is material in a criminal proceeding" is set forth at 18 U.S.C. 3144, "Release or detention of a material witness." The following questions pertain to the use of that provision in counterterrorism investigations and prosecutions during the period of time from September 11, 2001 to the present.

a. In how many cases have the authorities of 18 U.S.C. 3144 been used?

b. How many individuals are currently detained under the authority of 18 U.S.C. 3144?

c. In how many cases where the authority of 18 U.S.C. 3144 has been used has the individual arrested and detained in fact testified in "a criminal proceeding."

d. 18 U.S.C. 3144 prohibits the detention of any individual where "testimony of such witness can adequately be secured by deposition." In how many cases where the authority of 18 U.S.C. 3144 has been used has a deposition been taken and the witness released?

e. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 3144 has the witness been subsequently charged with a crime?

f. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 3144 has the witness be subsequently transferred to the custody of the Department of Defense? Please describe the facts and circumstances of each such case.

g. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 3144 has the witness be subsequently transferred to the custody of a foreign government? Please describe the facts and circumstances of each such case.

Response

h. What procedures and safeguards are in place to ensure that the authorities of 18 U.S.C. 3144 are not being used for purposes of preventive detention, or to hold individuals suspected of criminal activity without charging them with the commission of a crime? b5

Response:

[redacted]

i. What written policies or directives of the Department of Justice or the Federal Bureau of Investigation govern the application of the authorities set forth in 18 U.S.C. 3144? b5

Response: [redacted]

81. In briefs filed with the Supreme Court in the matter of Padilla v. Rumsfeld, as well as in related cases and in public statements, the President and the Attorney General have asserted that the President, in his capacity as Commander-in-Chief may detain individuals, including United States citizens, as "enemy combatants." The following questions pertain to the exercise of this authority during the period from September 11, 2001 to present.

a. What role has the Federal Bureau of Investigation played in the arrest, detention, and interrogation of individuals held in custody pursuant to this authority as "enemy combatants?"

Response: (Reassigned to CTD)

b. How many individuals have been arrested or detained pursuant to this authority?

c. How many United States citizens have been arrested or detained pursuant to this authority?

d. How many United States persons, as defined in Executive Order 12333, Section 3.4(i), and excepting United States citizens, have been arrested or detained pursuant to this authority?

Response: [redacted] b5

[redacted]

e. What rules, procedures or practices govern the conditions of confinement and the methods of interrogation used in cases where an individual has been arrested or detained pursuant to this authority? b5

Response: [redacted]

83. Sections 201 and 202 of the USA-Patriot Act added a number of offenses to the "predicate offense list" applicable to criminal wiretaps pursuant to Chapter 119 of Title 18. The following question pertains to the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. In how many cases has have the newly-added predicate offenses been used to support an application for a criminal wiretap under the authority of Chapter 119 of Title 18?

Response: [redacted]

b. In how many such cases has the newly-added predicate offense been the only predicate offense asserted as the basis for the warrant, i.e., where a warrant could not have been lawfully issued but for the passage of the additional criminal predicates? b5

Response: [redacted]

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute, including the addition of predicate crimes, which the Congress should consider?

Response: Sections 201 and 202 of the USA Patriot Act are currently scheduled to expire at the end of 2005.

b5

87. Section 209 of the USA-Patriot Act clarified the law with regard to the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. How many such search warrants have been issued since

passage of this act?

Response:

b5

b. In such cases, have there been any instances in which a wiretap, as opposed to a search, warrant would not have been supported by the facts asserted in support of the search warrant.

Response: This information is unavailable for the same reasons stated above. It is clear, however, that the requirements to obtain an federal wiretap are considerably greater than those for a search warrant.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

b5

[redacted] b5

95. Section 225 of the USA-Patriot Act provides immunity for those who aid in the execution of a FISA order. Has such immunity been invoked?

Response: No; with respect to FBI investigations, immunity has not been claimed under this section in either the civil or criminal context.

Brandon Mayfield Fingerprint Identification and Detention

101. On May 24th, a federal court dismissed the material witness proceeding against Brandon Mayfield, an attorney and former U.S. Army officer. In written submissions to the court and in public statements the FBI has admitted that the fingerprint of Mayfield was mistakenly matched to a fingerprint recovered at the scene of the May 11, 2004, Madrid train bombing.

d. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

Response: [redacted] b6 b7C

Use of the USA PATRIOT Act

102. In October 2003, the Department reported that as of April

1, 2003, it had sought, and courts had ordered, delayed notice warrants 47 times.

a. As of the date of your response to these questions, or some reasonable recent date, how many times has the Department sought and received authorization to execute a delayed notification search since enactment of the PATRIOT Act?

Response: The number of delayed notice search warrants reported in April 2003 was compiled by the Executive Office of United States Attorneys (EOUSA) through a field survey of U.S. Attorney's Offices. It is our understanding that EOUSA is currently updating that figure with another survey. When that figure is made known to the FBI, it will be provided.

b. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "seriously jeopardized an investigation"? For each such delayed notice warrant, please describe how granting contemporaneous notice would have seriously jeopardized the investigation and please indicate whether seriously jeopardizing the investigation was the sole basis or one of multiple grounds for delaying notice.

c. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "unduly delayed a trial"? For each such delayed notice warrant, please describe how requiring contemporaneous notice would have unduly delayed a trial and please indicate whether unduly delaying a trial was the sole basis or one of multiple grounds for delaying notice.

Response (b. and c.):

b5

d. How many of the delayed notice warrants were issued with a (i) seven-day or less delay; (ii) 8 to 30 day delay; (iii) 31

to 60 day delay; and (iv) time period of 61 days or more and what were those time periods?

e. How many of the delayed notification warrants issued since the PATRIOT Act was passed were used in non-terrorism criminal matters?

f. Please provide the case name, docket number, and court of jurisdiction for each case in which a delayed notice warrant was issued since enactment of the PATRIOT Act.

Response

b5

Message From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Tuesday, August 31, 2004 5:53 AM
To: [redacted] OCA) (FBI) b6
Cc: [redacted] (OGC) (FBI) [redacted] OGC) (OGA); KELLEY, b7C
PATRICK W. (OGC) (FBI)
Subject: RE: PLEASE DELETE LAST MESSAGE. NSLB RESPONSES WITH CTD INPUT

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I'll do what I can, but OGC is not the place to answer most of this. 84b(i) and 84c look fine to me, but OGC is not in the loop for the activity represented. I don't have the questions so don't know what the others are (I'll check with [redacted] here), but, as you know, we don't run cases either so what the field does is often unknown to us, or anyone at HQ.

-----Original Message-----
From: [redacted] (OCA) (FBI) b6
Sent: Monday, August 30, 2004 5:37 PM b7C
To: BOWMAN, MARION E. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (OGA); KELLEY,
PATRICK W. (OGC) (FBI)
Subject: RE: PLEASE DELETE LAST MESSAGE. NSLB RESPONSES WITH CTD INPUT

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Spike. Thanks. I had previously received much of this, but this does fill in a few gaps.

Here's where we stand.

1. This document provides the following answers for the first time.
   84b(i) (which has several subparts)
   84c (which has several subparts)
I need approval of these answers by a DAD (or equivalent) or higher. Do we have a demonstration that these were approved by [redacted] If not, could you review them and forward b6
to me your approval (email is fine)? b7C

2. I still need responses to the following:
   88a, b, d
   91a, b
   93a, c
A couple of these questions (such as # 88a) request numbers of cases, which I understand we may not keep. If you let me know that, I can try to deal with those. I do, however, need the rest of the responses. For example, while 88a asks for the number of cases in which we've used Section 212 of the Patriot Act (which we may not be able to answer), 88b asks for cases in which

we needed Patriot Act authority for a reason other than time constraints, and 88d asks if we want changes to 212.

I know inflicts incredible pain and agony. Does it help that I find this painful as well?

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]
b2
b6
b7C

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Monday, August 30, 2004 4:47 PM
To: [redacted] OCA) (FBI)
Cc [redacted] (OGC) (FBI) [redacted] (OGC) (OGA); KELLEY, PATRICK W. (OGC) (FBI)
Subject: FW: PLEASE DELETE LAST MESSAGE. NSLB RESPONSES WITH CTD INPUT

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I thought these had been forwarded already, but in case not, here they are.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE HEARING
NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?

b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

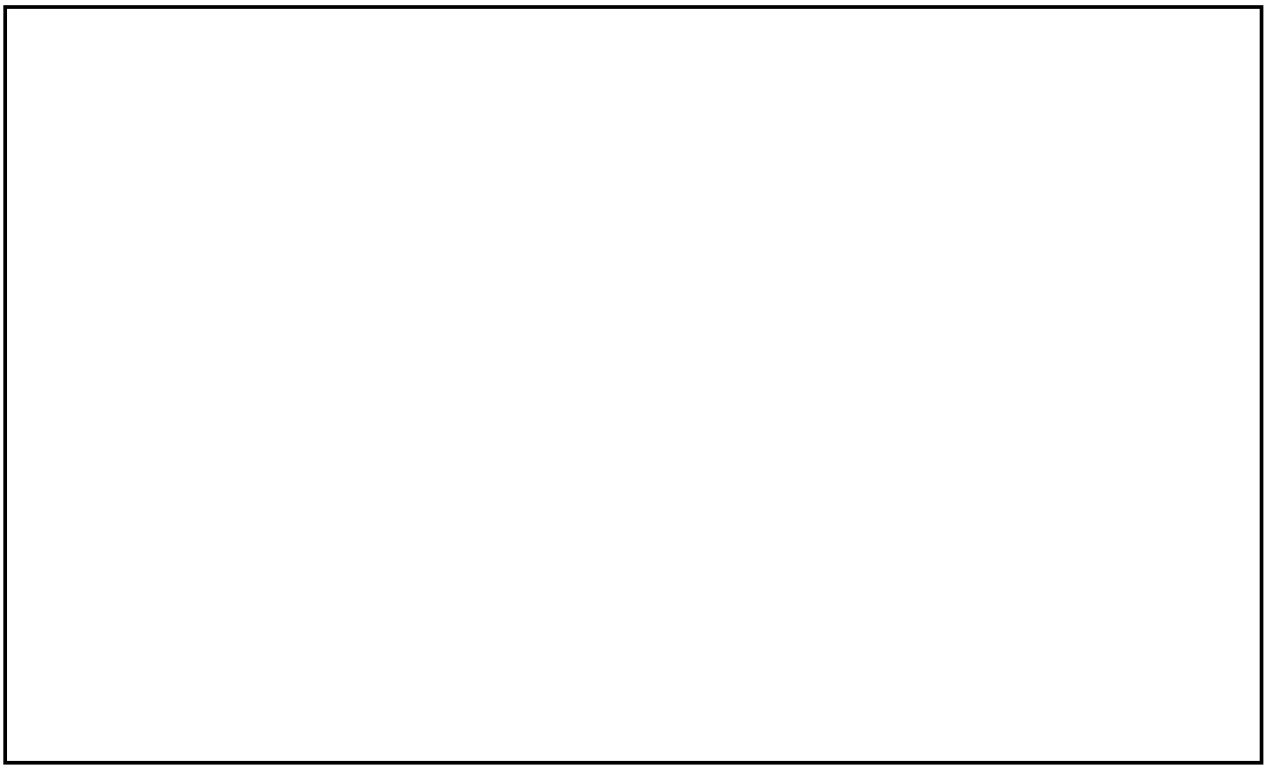
34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors. [redacted] b5

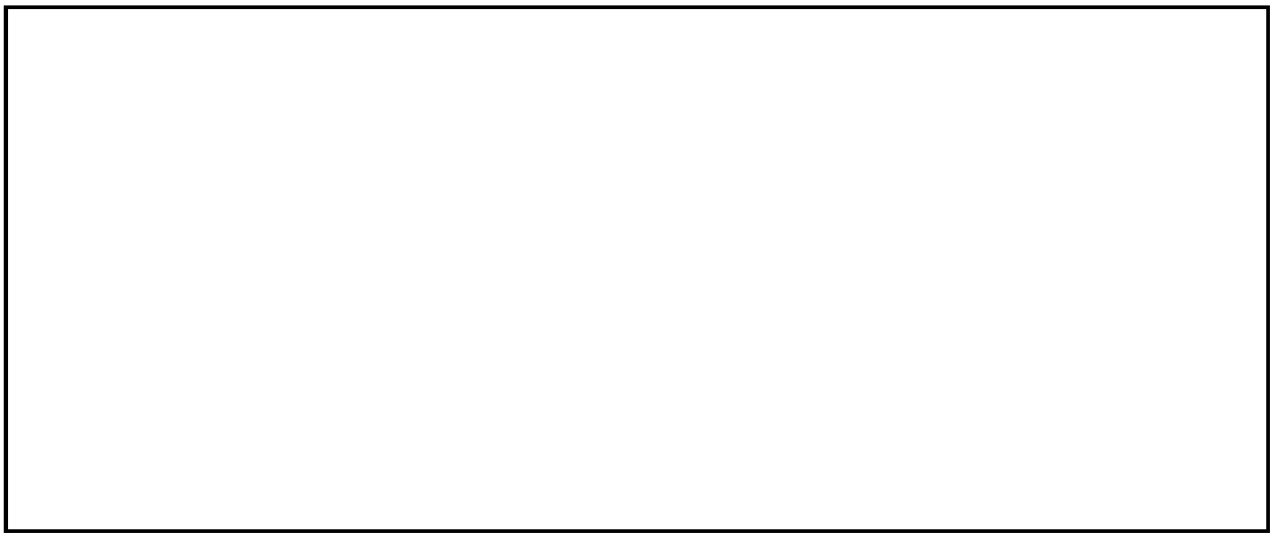
For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

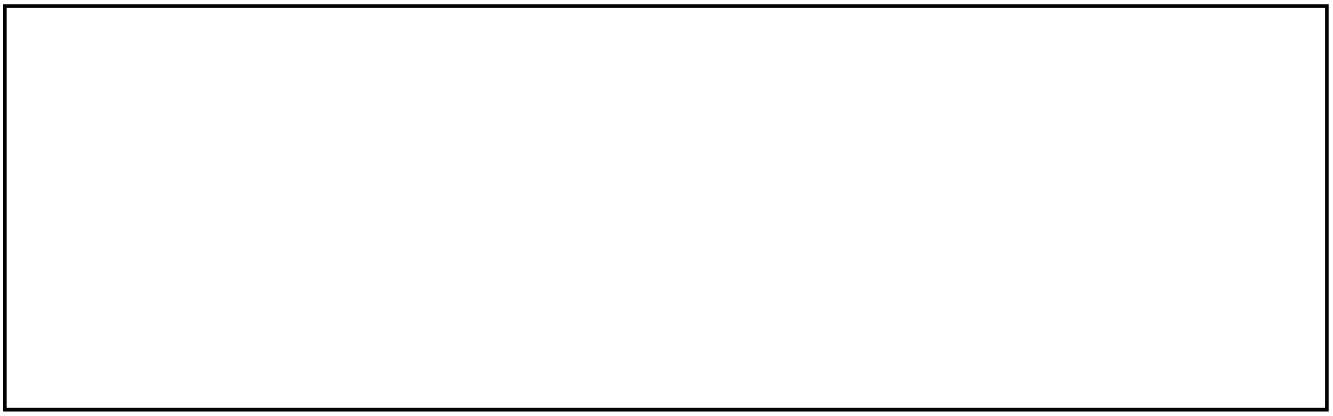
a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?



b5



b5



b5

b5

How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

b5

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing.

b5

b5

55. CTD. (Follow-up to Leahy 15) What specific policy changes have you made in response to the Inspector General's report on 9/11 detainees?

OCA Note: To assist CTD in responding, we note that, in response to a Question for the Record regarding a 9/11 Detainee hearing, the FBI indicated that DOJ and DHS had signed a memorandum of understanding (MOU) related to information sharing and, as recommended by the Inspector General, the FBI was working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. We also indicated that we were working with DHS to establish criteria and procedures for future investigations of alien detainees, including circumstances where a large number of aliens with potential ties to terrorism are detained.

Response: The DOJ and DHS have signed a memorandum of understanding (MOU) relating to information sharing and the FBI is working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. DOJ is still working with DHS to draft an MOU to establish criteria and procedures for future investigations of alien detainees of national security interest. With respect to other policy changes, the FBI has worked to establish the Terrorist Screening Center (TSC) and TTIC, which will substantially improve the FBI's ability to obtain information about alien detainees from various agencies and process this information in a timely fashion. The FBI continues to work with the National Security Law Division, ICE, to review alien detainee cases of national security interest on a case-by-case basis.

58. OGC. (Follow-up to Leahy 18A) When will the FISA Management System (FISAMS) be fully operational? With whom is the contract for development of FISAMS? How much will it cost and what funds are being used to pay for it?

Response: The FISA Management System (FISAMS) became operational at the end of January 2004. The FBI trained the largest 13 FBI field offices on the system. These 13 offices are currently processing their FISA requests through the FISAMS,

extent permitted by the Constitution and the laws of the United States. In addition, as the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). b5 [redacted]

. In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other intitiatives, such as the Foreign Terrorist Tracking Task Force and the National Joint Terrorism Task Force have assisted in permitting better information flow with our law enforcement counterparts and will improve the handling of such cases. b5 [redacted]

82. OGC. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107- 56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeapor[dize] an investigation or unduly [delay] a trial" been used? Please describe the circumstances in each of these cases?

b5

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response: This information may be disseminated in any format deemed appropriate for the particular circumstances. [As to the sub questions below, OGC does not have information pertaining to electronic intelligence reports and refers OCA to CTD.]

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been

issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response: The information may be disseminated in any format deemed appropriate for the circumstances. [OGC would refer the remaining sub-parts to CTD for a response as to how they are disseminating this information.]

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response: On September 23, 2002, the Attorney General promulgated guidelines that established procedures for the disclosure of information under Section 905(a) of the USA-Patriot Act. A copy of the procedures is attached as well as the Office of the General Counsel's EC advising all Divisions of these procedures. The Attorney General also promulgated guidelines under Section 905(b) of the USA Patriot Act (see attached). OGC is not aware of procedures established under Section 905(c) of

the USA-Patriot Act and would refer this question to DOJ.

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b5

Response: [redacted] **OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information. [Note: DOJ has provided or is in the process of providing examples of how the Patriot Act has been an asset to our investigations and why the sunset provisions should not sunset. We refer OCA to the DOJ for these examples.]**

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

b5

[redacted]

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

b5

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. [redacted]

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community, [redacted]

b5 **through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins.**

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence. [redacted]

Intelligence

b5 **Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.**

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism

Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners, [redacted]

b5

In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, [redacted] **access and responsiveness to local FBI field office, FBI program and national intelligence requirements . The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.**

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during

the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

[redacted] b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

b5

[redacted]

(i) How many of such cases were terrorism-related?

b5

[redacted]

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application

of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation

received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b1
b2
b7E

Response:

a

(S)

b

(S)

b5

(U)

b2
b5
b7E

b2
b7E

(U)

b5

(U)

(S)

b1
b2
b7E

b5

[redacted] b5

e. QUESTION RE "ELECTRONIC INTELLIGENCE REPORTS" - PLEASE REFER TO CTD.

f. FOR INSPECTION DIVISION

[redacted] b5

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation

of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b5

b5

[redacted] b5

[redacted] b5 b1 b7A (S)

[redacted] b5 b7A b6 b7C

b5
b6
b7C
b7A

b5
b7A

b1
b5
b7A

b5

b5
b6
b7C

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

b5

101 d. OGC. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

[redacted]

b6
b7C

100 e. CTD (in coordination with OGC). Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.

b1
b5
b6
b7C

[redacted] (S)

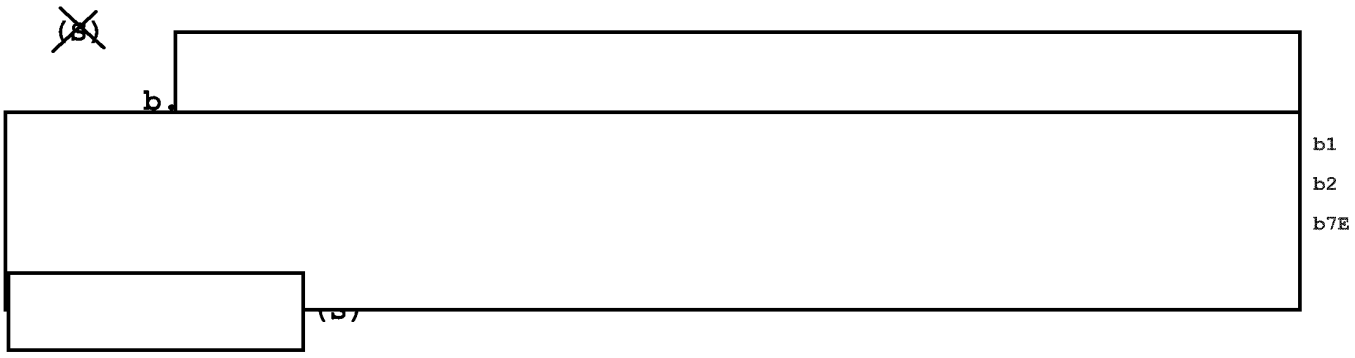
103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

b1
b2
b7E

Response: a. [redacted] (S)


~~(S)~~
b
b1
b2
b7E
(S)

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 26
Page 428 ~ Duplicate
Page 429 ~ Duplicate
Page 430 ~ Duplicate
Page 431 ~ Duplicate
Page 432 ~ Duplicate
Page 433 ~ Duplicate
Page 434 ~ Duplicate
Page 435 ~ Duplicate
Page 436 ~ Duplicate
Page 437 ~ Duplicate
Page 438 ~ Duplicate
Page 439 ~ Duplicate
Page 440 ~ Duplicate
Page 441 ~ Duplicate
Page 442 ~ Duplicate
Page 453 ~ Duplicate
Page 454 ~ Duplicate
Page 455 ~ Duplicate
Page 456 ~ Duplicate
Page 457 ~ Duplicate
Page 458 ~ Duplicate
Page 459 ~ Duplicate
Page 460 ~ Duplicate
Page 461 ~ Duplicate
Page 462 ~ Duplicate
Page 463 ~ Duplicate

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 12/11/2001

To: All Field Offices

Attn: ADIC; SAC; CDC
FCI/IT Supervisors

Counterterrorism

AD Watson; DADSs
Section Chiefs

National Security

AD Gallagher; DADs
Section Chiefs

From: General Counsel
National Security Law Unit, Room 7075
Contact: [redacted] b6 b7C

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E

Drafted By: [redacted] b6 b7C

Case ID #: 66F-HQ-A1255972

Title: NATIONAL SECURITY LETTER MATTERS

Synopsis: Provides guidance on the preparation, approval, and service of National Security Letters (NSLs).

Reference: 66F-HQ-A1255972 Serial 15

Enclosure(s): 1) Subscriber Information NSL Model
2) Toll Billing Records NSL Model
3) Electronic Subscriber Information NSL Model
4) Electronic Communication Transactional Records NSL Model
5) Financial Records NSL Model
6) Identity of Financial Institutions NSL Model
7) Consumer Identifying Information NSL Model
8) Subscriber/Electronic Subscriber (EC) Model
9) Toll/Transactional Records EC Model
10) Financial Records EC Model
11) Financial Institutions/Consumer Identity EC Model
12) ECPA NSL Checklist
13) RFPA NSL Checklist
14) FCRA NSL Checklist

Details: In the referenced communication, dated 11/09/2001, the Director of the FBI delegated the authority to certify NSLs to the following officials: (1) the Deputy Director; (2) The Assistant Directors (ADs) and all Deputy Assistant Directors (DADs) of the Counterterrorism Division (CTD)

and the National Security Division (NSD); (3) the General Counsel and the Deputy General Counsel for National Security Affairs (DGC), Office of the General Counsel (OGC); (4) the Assistant Director in Charge (ADIC), and all Special Agents in Charge (SACs), of the New York, Washington, D.C., and Los Angeles field divisions; and (5) the SACs in all other field divisions. The purpose of this electronic communication is to provide comprehensive guidance on the preparation, approval, and service of NSLs.

1. Introduction to National Security Letters

NSLs are administrative subpoenas that can be used to obtain several types of records. There are three types of NSLs. First, pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, the FBI can issue NSLs for: (1) telephone subscriber information (limited to name, address, and length of service); (2) telephone local and long distance toll billing records; and (3) electronic communication transactional records. Second, pursuant to the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5), the FBI can issue NSLs to obtain financial records from banks and other financial institutions. Finally, pursuant to the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u, the FBI can issue NSLs to obtain consumer identifying information and the identity of financial institutions from credit bureaus.

NSLs are tools available in investigations conducted under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). The FCIG currently provide that an NSL can be issued during the course of a full international terrorism or foreign counterintelligence investigation. **NSLs cannot be used in criminal investigations unrelated to international terrorism or clandestine intelligence activities.** Given the new statutory language, the OGC and DOJ have taken the position that NSLs also may be authorized in foreign counterintelligence (FCI) and international terrorism (IT) preliminary inquiries (PIs), with prior coordination through the relevant NSD or CTD unit at FBIHQ. This position is based on the conclusion that all investigations authorized under the FCIG, including PIs, are to "protect against international terrorism or clandestine intelligence activities," as required by the NSL statutory authorities. At present, however, issuing an NSL in the context of a PI will require a waiver or modification of the FCIG. Obtaining such a waiver currently is possible only in international terrorism cases. The FCIG are being revised, but this revision may take some time. Thus, whenever the information sought is relevant to an established full investigation, the field likely will find it more efficient to issue an NSL out of the related full investigation than to request one in a PI.

2. General Policy on the Use of NSL Authority

NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information. However, they must be used judiciously. The USA PATRIOT Act greatly broadened the FBI's authority to gather this information. However, the provisions of the Act relating to NSLs are subject to a "sunset" provision that calls for the expiration of those provisions in four years. In deciding whether or not to re-authorize the broadened authority, Congress certainly will examine the manner in which the FBI exercised it. Executive Order 12333 and the FCIG require that the FBI accomplish its investigations through the "least intrusive" means. Supervisors should keep this in mind when deciding whether or not a particular use of NSL authority is appropriate. The greater availability of NSLs does not mean that they should be used in every case.

In addition, the removal of any requirement for FBIHQ coordination in the issuing of NSLs creates the possibility of duplicate requests for the same information by different field offices. Field offices must take steps to avoid this. In particular, the field should check FBI databases (ACS, Telephone Application, etc.) and open sources to see if the information sought has already been obtained by the FBI or whether it is publically available. This is particularly important when considering issuing NSLs for telephone or electronic communications data under the Electronic

Communications Privacy Act (ECPA). Unlike the criminal authorities in ECPA, the NSL authority does not require the government to reimburse carriers or Internet Service Providers (ISPs) for the cost of producing the requested information. A dramatic increase in duplicate NSLs will only augment existing pressure to require governmental reimbursement.

Individual field offices have the responsibility for establishing and enforcing an appropriate review and approval process for the use of NSL authorities.

3. The Mechanics of Producing NSLs

For all types of NSLs, the issuing office needs to prepare two documents: (1) the NSL itself; and (2) an EC approving the NSL and documenting the predication. Model NSLs and ECs for all variations of the three types of NSLs are included as attachments to this communication. These materials will also be placed on the NSLU Intranet Website and will be distributed by GroupWise e-mail. Once the initial implementation of these new authorities is accomplished, NSLU will work to develop a macro or form to further streamline the NSL process.

A. The NSL

There are presently seven variations of the three NSL types: 1) subscriber information; 2) toll billing records; 3) electronic subscriber information; 4) electronic communication transactional records; 5) financial records; 6) identity of financial institutions; and 7) consumer identifying information. This section will discuss the features that these variations share in common and highlight the differences.

All NSLs must be addressed to an appropriate company point of contact. NSLU will place a list of known points of contact on its intranet website. However, the responsibility for ensuring that the company point of contact is up to date belongs to the drafting field division. Field divisions should advise NSLU of any new points of contact, or when a particular point of contact is no longer valid. Please note that the company point of contact address does not include a zip code, because NSLs must be hand-delivered.

The first paragraph of every NSL provides the appropriate statutory authority for the request, identifies the types of records requested, and provides available identifying information so that the company can process the NSL request. It is this first paragraph that contains the differences that warrant the seven NSL varieties.

Subscriber and electronic subscriber NSLs should have a specific date for each of the phone numbers/e-mail addresses requested. Typically, the specific date is going to be the date that the phone number or e-mail address was used in communication with the subject of the investigation. Any phone numbers identified in a subscriber request should contain all ten digits of the phone number, including the area code.

Toll billing record and electronic communication transactional record requests should have a range of dates for each of the phone numbers/e-mail addresses requested. The date range may be from inception to present, or some other specified date range relevant to the investigation. Any phone numbers identified in a toll billing record request should contain all ten digits of the phone number, including the area code.

Financial record requests should include all available identifying information to facilitate the financial institution's records search. Typically, such identifying information includes: name, account numbers, social security number, and date of birth. The time period for financial record requests is typically from inception of account(s) to present, although a more specific date range may be used.

Credit record requests are similar to financial requests in that they should include available identifying information to facilitate the credit agency's records search. Typically, such identifying information includes: name, social security number, and date of birth. There is no need to specify a date range for credit record requests because these requests seek all records where the consumer maintains or has maintained an account.

The second paragraph of every NSL contains the statutorily required certification language. The certification language is virtually identical for every NSL. However, please note that the certification language used in the financial records NSLs is slightly different than the others in that it states "the records are sought for foreign counterintelligence purposes . . . ." Financial records also contain an additional certification that the FBI has complied with all applicable provisions of the RFPA. Use of the model NSLs will ensure that the proper certifications are made.

The next paragraph contains an admonition for the phone company, ISP, financial institution, or credit agency receiving the NSL. The paragraph warns that no officer, employee, or agent of the company may disclose that the FBI has sought or obtained access to the requested information or records.

The last substantive paragraph instructs the company point of contact to provide the records personally to a representative of the delivering field division. It also states that any questions should be directed to the delivering field division. This last paragraph requires the person preparing the NSL to input the appropriate delivering field division in two places.

The model NSLs for financial records and electronic communication transactional records each have a separate attachment. These attachments provide examples of information which the company might consider to be financial or electronic communication transactional records.

Finally, the NSL is an unclassified document because it does not detail the specific relevance of the requested records to an authorized FBI investigation. There is no need to classify the NSL when attaching it to the cover EC.

B. The Cover EC

The Cover EC serves four essential functions in the NSL process: (1) it documents the predication for the NSL by recording why the information sought is relevant to an investigation; (2) it documents the approval of the NSL by relevant supervisors and the legal review of the document; (3) it contains the information needed to fulfill the Congressional reporting requirements for each type of NSL; and (4) it transmits the NSL to the requesting squad or delivering field division for delivery to the appropriate telecommunications carrier, ISP, financial institution, or credit agency. There are four varieties of model ECs provided with this communication: (1) subscriber/electronic subscriber information; (2) toll billing/electronic communication transactional records; (3) financial records; and (4) credit information. When preparing an NSL request, the field should use one of these model ECs, giving special consideration to the elements discussed in this section.

1) Field Descriptors

This section will generally explain how most of the EC field descriptors should be completed. The "**Precedence**" descriptor will typically be "ROUTINE." The "**Date**" descriptor should reflect the date the NSL and the EC were approved. The "**To**" descriptor will always include "General Counsel" and the requesting squad's field division. It may also include the name of the delivering field division (always Los Angeles in the case of FCRA NSLs) and the office of origin, if applicable. The "**Attn**" descriptor should include the name of the Chief, NSLU, and the squad supervisors and case agents from the requesting squad, delivering field division, and office

of origin, if applicable and if known. The credit model EC identifies the FBI personnel working on Squad 4, Santa Ana RA, who are currently responsible for the service of FCRA NSLs. The "**From**" descriptor should identify the certifying official's field division, and include the title of the certifying official. The "**Contact**" descriptor should reflect the name and phone number of the requesting squad case agent. The "**Drafted By**" descriptor should reflect the name of the person who prepared the NSL package. The "**Case ID #**" descriptor must contain the case file number relevant to the request, and the case file numbers indicated in the model EC. The "**Title**" descriptor should list the subject's name, any known aliases, whether the investigation is an FCI or IT investigation directed at a particular foreign power, and identify the office of origin, e.g., WILLIAM BADGUY, AKA BILL BADGUY, FCI-IRAQ, OO: NEW YORK. The "**Synopsis**" descriptor should use the standard boilerplate contained in the appropriate model EC. The "**Derived From**" descriptor should be "**G-3**" in bold typeface. The "**Declassify On**" descriptor should be "**X1**" in bold typeface. the "**Full Investigation Instituted**" descriptor should contain the date the full FCI or IT investigation was opened on the subject and indicate whether the subject is a U.S. person. Please note that the word "**Field**" has been deleted from the field descriptor contained in the standard EC macro. In the unlikely event that an NSL is issued during a PI with prior FBIHQ approval, the field descriptor should be edited to state "**Preliminary Inquiry Instituted**." The remaining descriptors can be filled in according to the model EC being used.

2) Predication and Relevance

The USA PATRIOT Act has greatly simplified the NSL process. The FBI official authorizing the issuance of an NSL is no longer required to certify that there are specific and articulable facts giving reason to believe that the information sought pertains to a foreign power, or an agent of a foreign power. NSLs may now be issued upon a certification of relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

Accordingly, the first paragraph in the "Details" section of the EC should contain the predication for the full investigation and identify the relevance of the requested records to the investigation. Both the predication and relevance should be stated clearly and concisely. The predication should track with the predicates contained in FCIG, Section III.C.1. For example, the predication might state, "A full foreign counterintelligence investigation of subject, a Non-U.S. person, was authorized in accordance with the Attorney General Guidelines because he may be a suspected intelligence officer for the Government of Iraq." Another example might state, "A full international terrorism investigation of subject, a U.S. person, was authorized in accordance with the Attorney General Guidelines because he may be engaged in international terrorism activities by raising funds for HAMAS."

The relevance requirement ties the requested records to the appropriate full investigation. For example, relevance could be established by stating, "This subscriber information is being requested to determine the individuals or entities that the subject has been in contact with during the past six months." Another example might state, "The subject's financial records are being requested to determine his involvement in possible HAMAS fund raising activities."

3) Approval

The second paragraph in the "Details" section and the "Approved By" descriptor field of the EC should reflect the level of the official approving the issuance of the EC and signing the NSL's certification. Prior to certification, every NSL and cover EC issued by the field division should be reviewed by the squad supervisor, the Office of the Chief Division Counsel, and the ASAC. Lawyers reviewing NSL packages should use the checklists provided with this communication to ensure legal sufficiency. The last step in the approval process occurs when the certifying official (Deputy Director, ADs, General Counsel, ADICs, DADs, DGC, or SACs) personally signs the NSL and initials the EC. Certifying officials may not further delegate signature authority.

4) Reporting Requirements

NSLU will continue to prepare the mandatory reports to Congress required for each NSL type. To ensure that NSLU receives sufficient information to prepare these reports, it is critical that the person preparing the NSL package follow the NSL and EC models very carefully. The second lead in every model EC requests NSLU to "record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs." NSLU will be able to compile the reporting data provided that the cover EC includes the case file number, the subject's U.S. person status, the type of NSL issued, and the number of phone numbers, e-mail addresses, account numbers, or individual records being requested in the NSL. Once NSLU has entered this reporting data into its NSL database, it will clear the lead set in the cover EC.

5) Transmittal

Often, the squad requesting the NSL will be able to hand-carry the NSL locally to the appropriate company point of contact. However, in many situations, the field division drafting the NSL will have to get it delivered by another field division. In these situations, the drafting division should attempt to identify the squad and personnel at the delivering field division who will be responsible for delivering the NSL. In the event that the office of origin is different than either the drafting division or delivering division, the person drafting the NSL package should ensure that the case agent from the office of origin receives a copy of the package. The first lead in the model ECs should direct the requesting squad or delivering field division to deliver the attached NSL. If the delivering division is different than the drafting division or the office of origin, then this first lead should also request the delivering division to submit the results to the drafting division and/or the office of origin.

4. NSL Preparation Assistance

Some field divisions may, for a variety of reasons, opt not to exercise their delegated authority to issue NSLs. Other field divisions may exceed their capacity to issue NSLs and seek assistance in handling the overflow. NSLU will continue to process any NSL request that it receives. Field divisions should send their requests directly to NSLU, with information copies to the FBIHQ substantive unit. Such requests must contain all the information identified in this communication as necessary to prepare the NSL package. NSLU anticipates that it will be able to process such requests within one to three business days.

Any questions regarding this communication may be directed to [redacted] NSLU, OGC, at [redacted]

b6
b7C

LEAD(s):

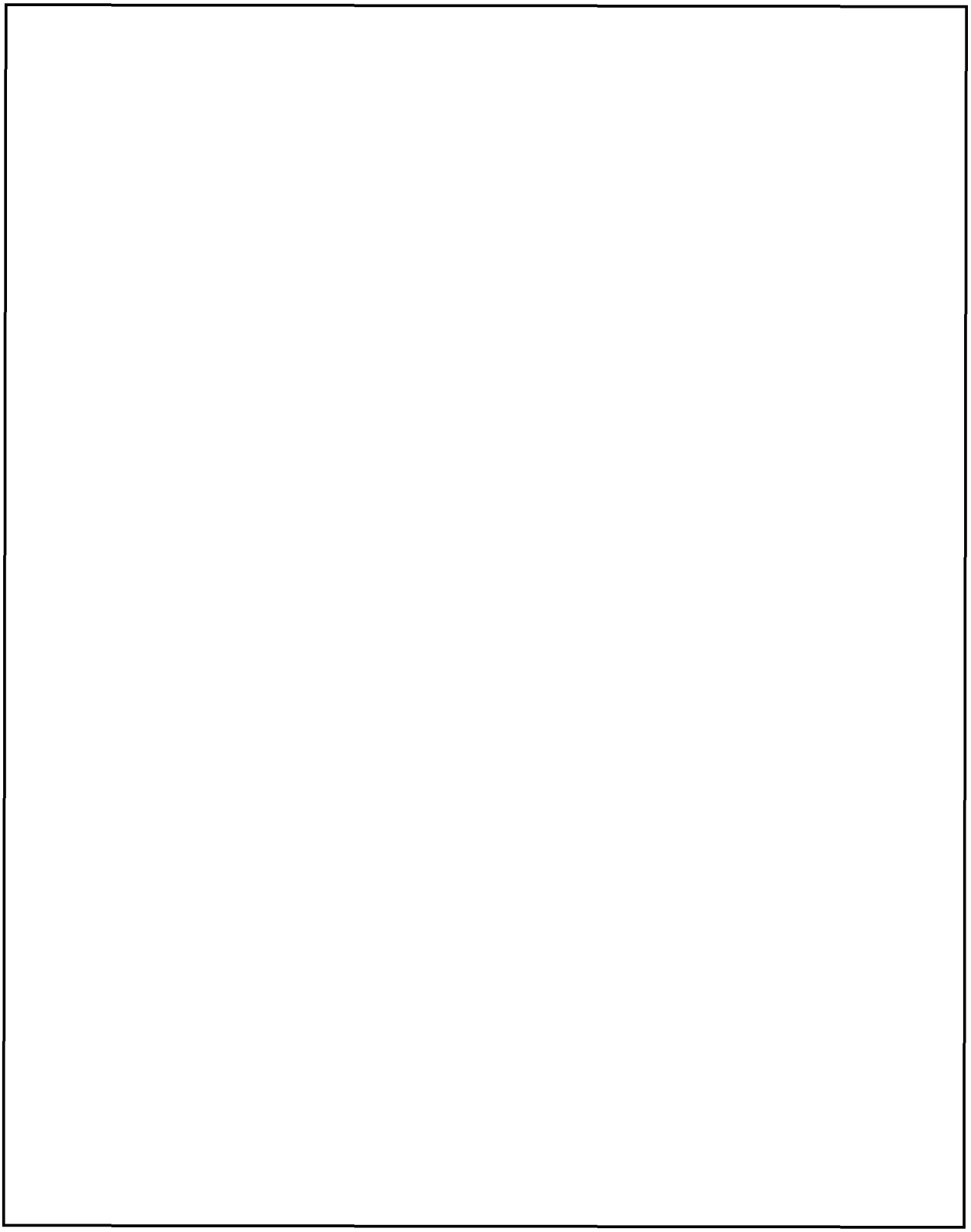
Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to all supervisory personnel involved in the National Security Letter process.

b5

b5
b6
b7C



b5
b2
b7D
b6
b7C
b7A

(S)

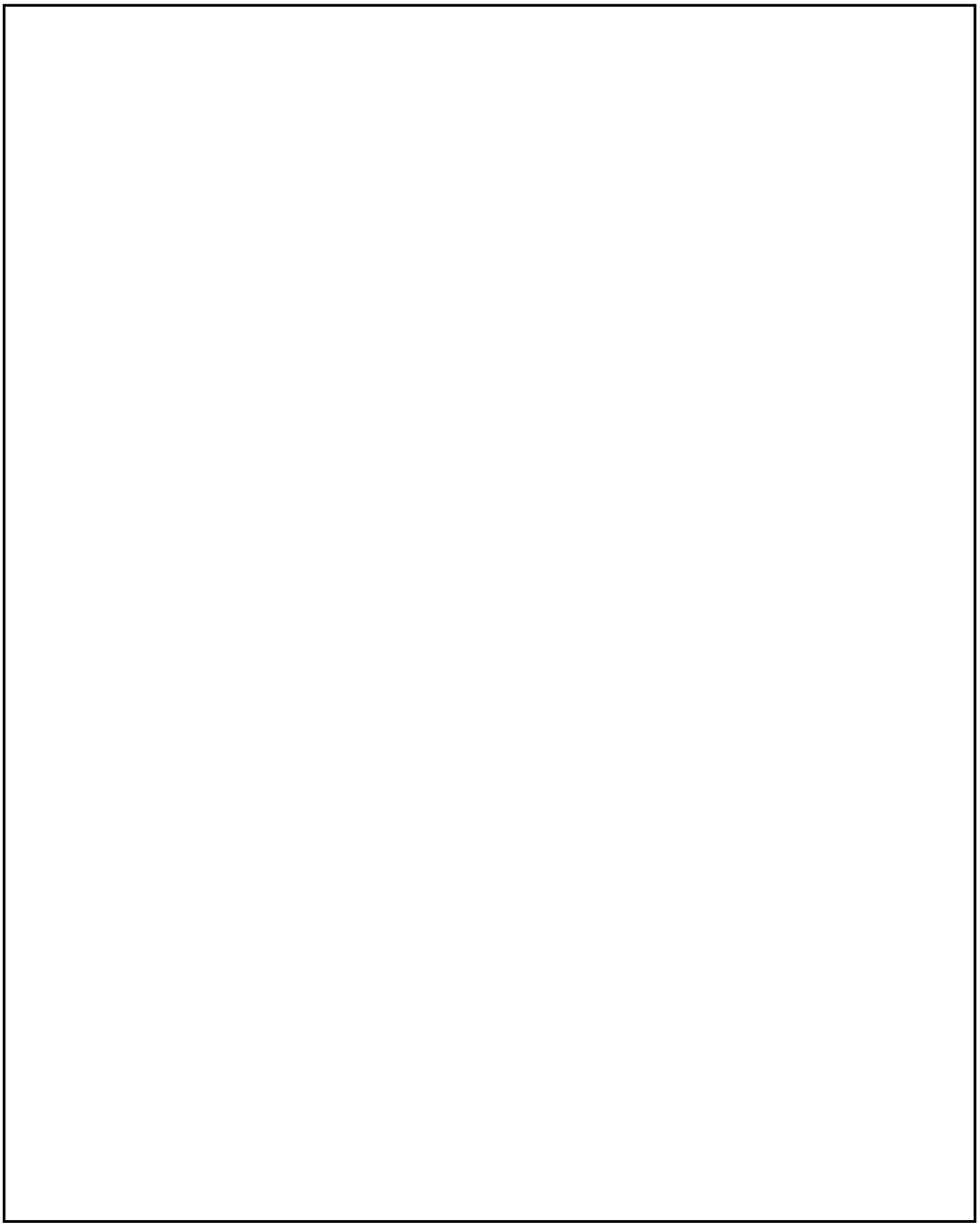
(S)

(S)

(S)

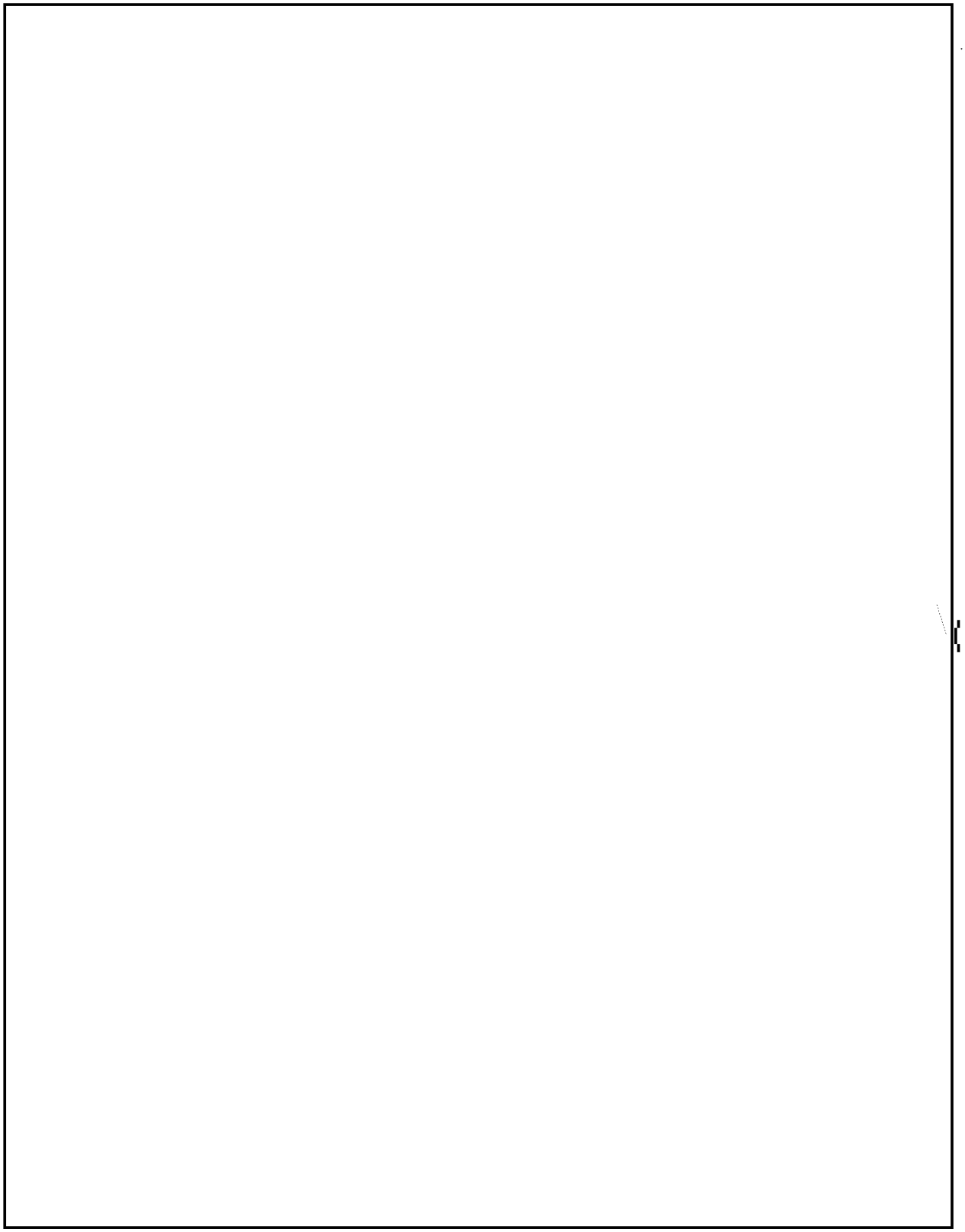
(S)

b5
b2
b7C
b1



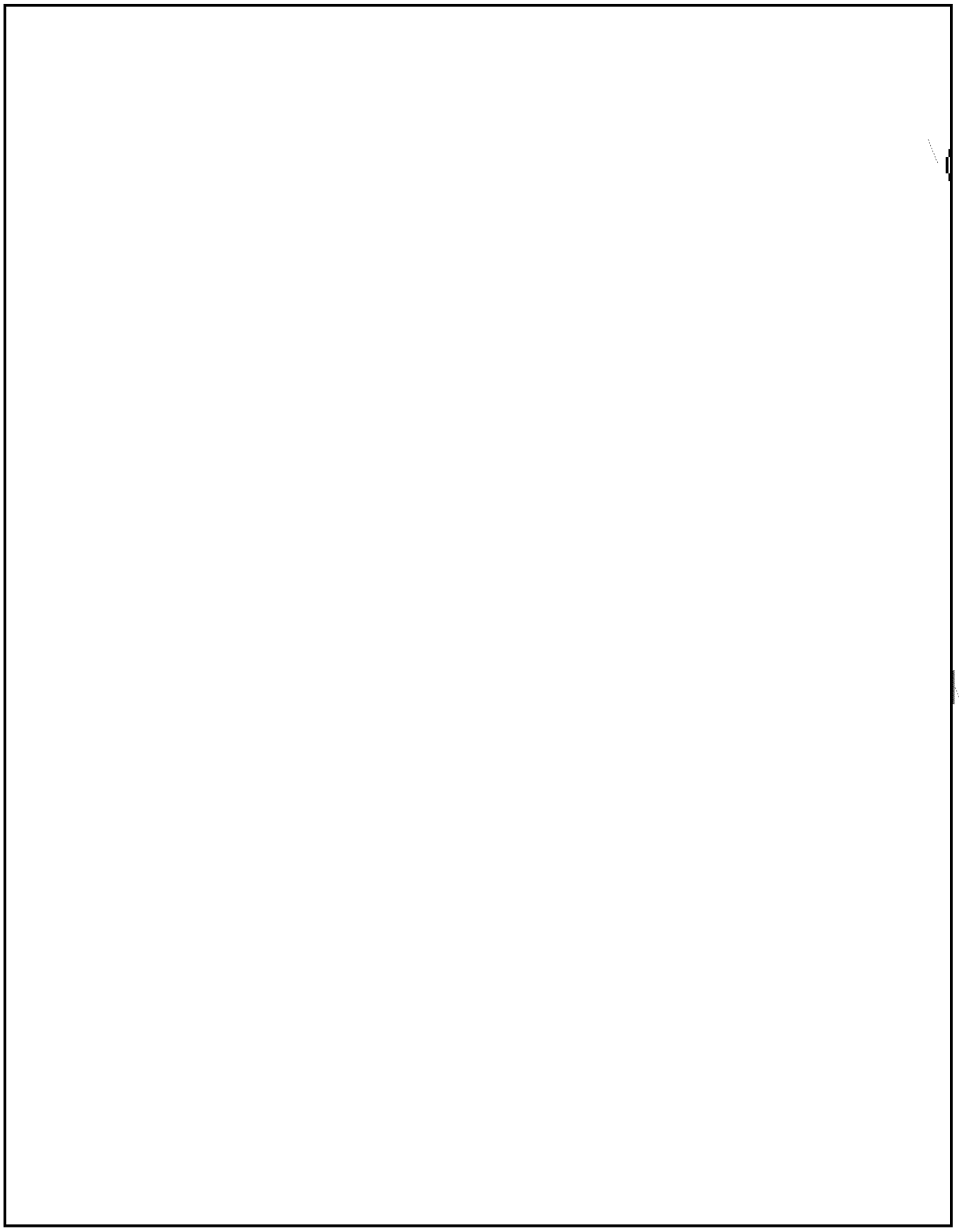
(S)

b5
b2
b7E
b1



b5
b2
b7E
b1

(S)



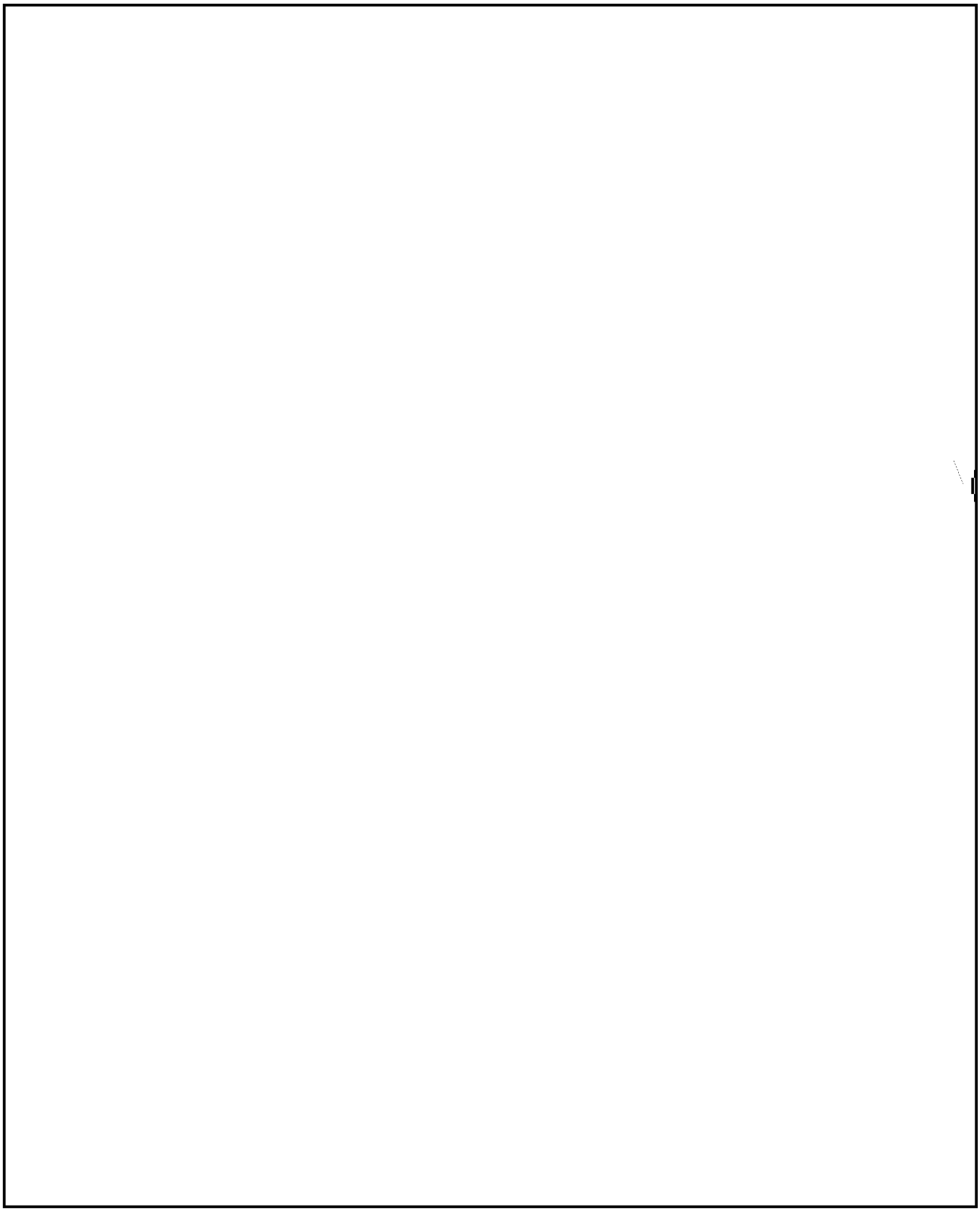
(S)

b5
b2
b7E
b1

(S)

b5
b2
b7E
b6
b7C

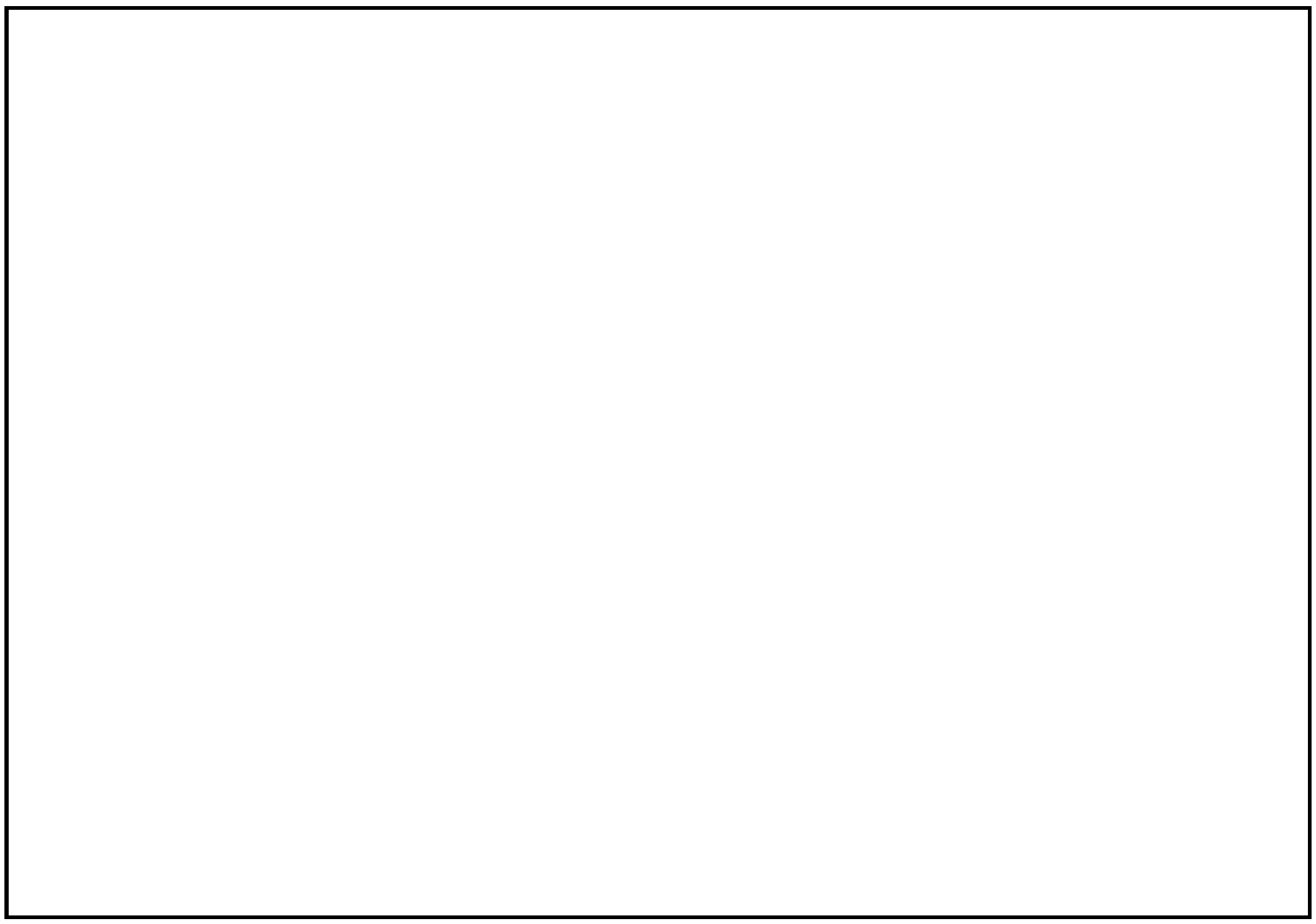
b5
b7A
b2
b7E



(S)

b5
b2
b7E
b1

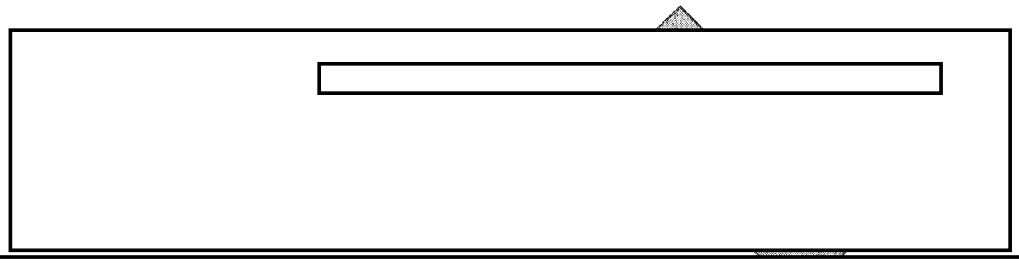
b5
b2
b7E
b7A



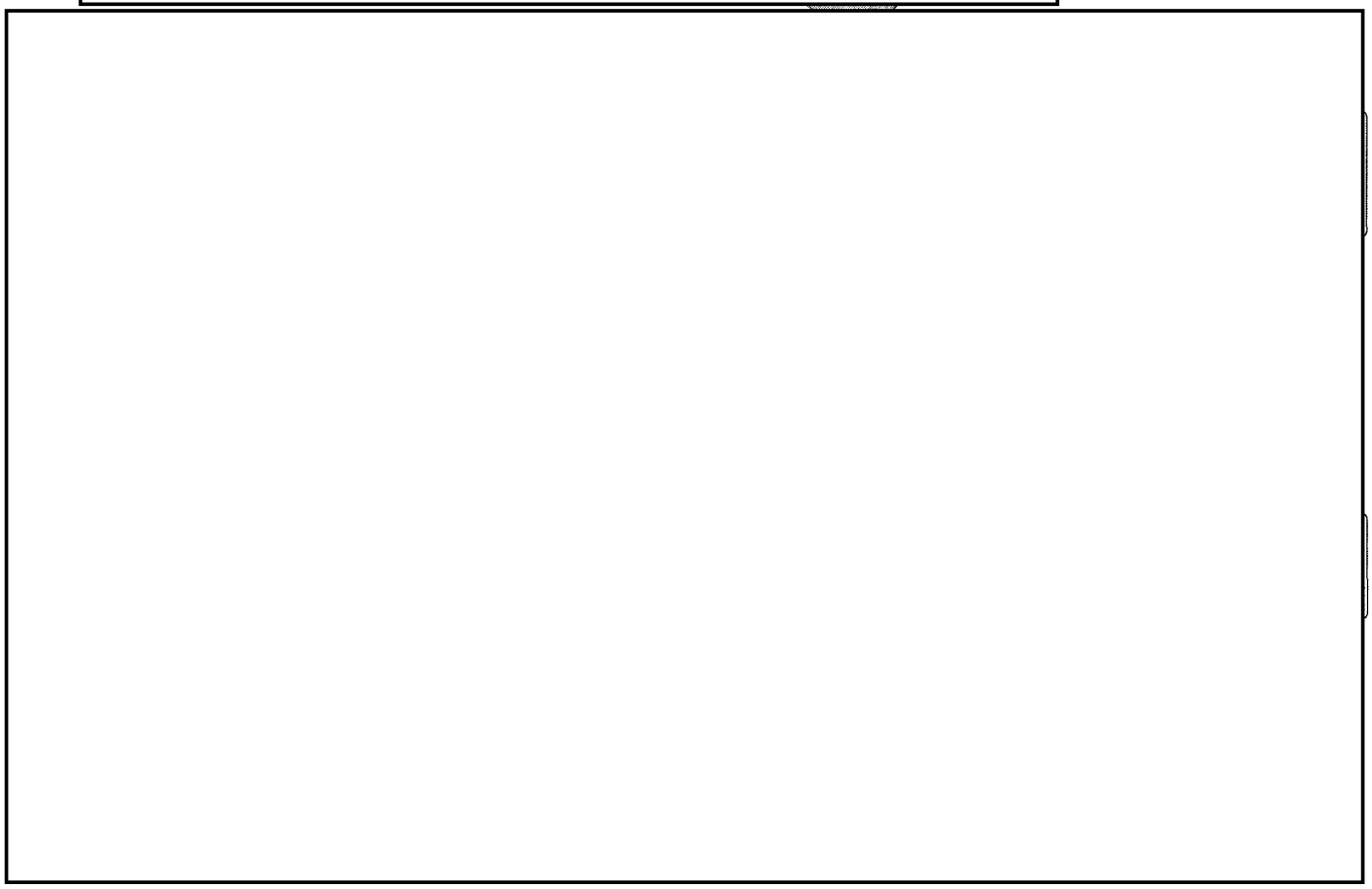
b5
b2
b7E

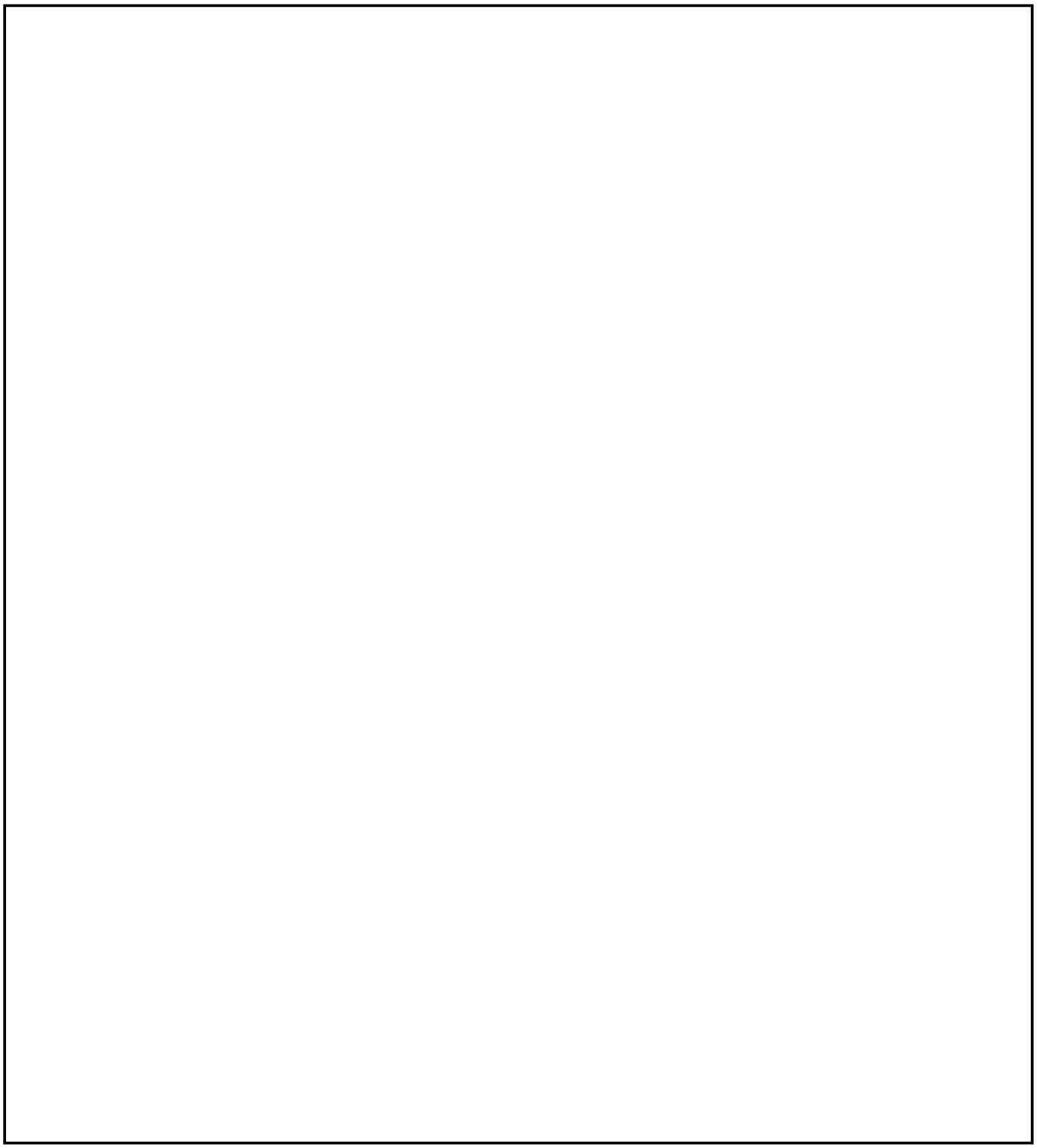
SECRET

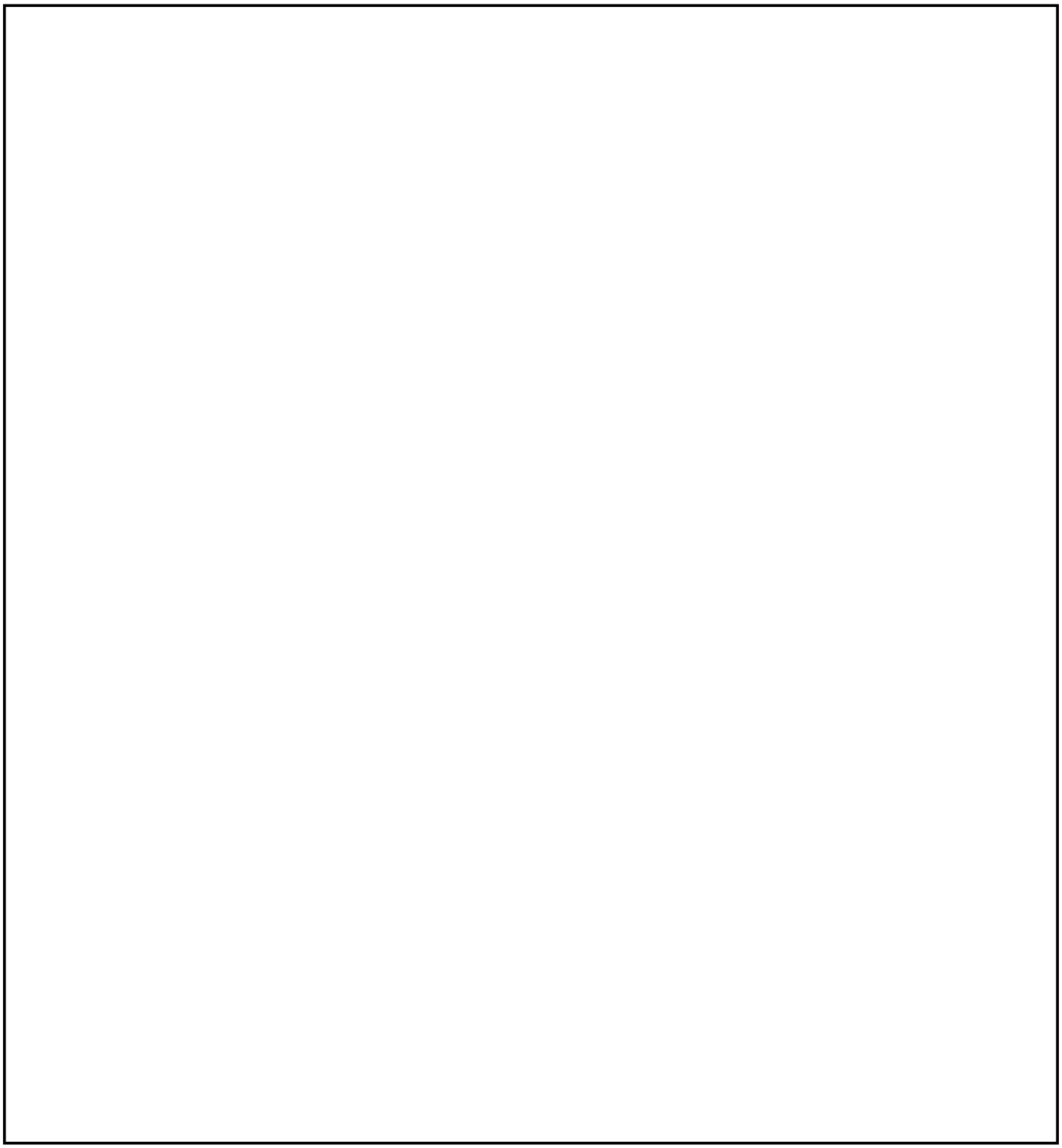
b5



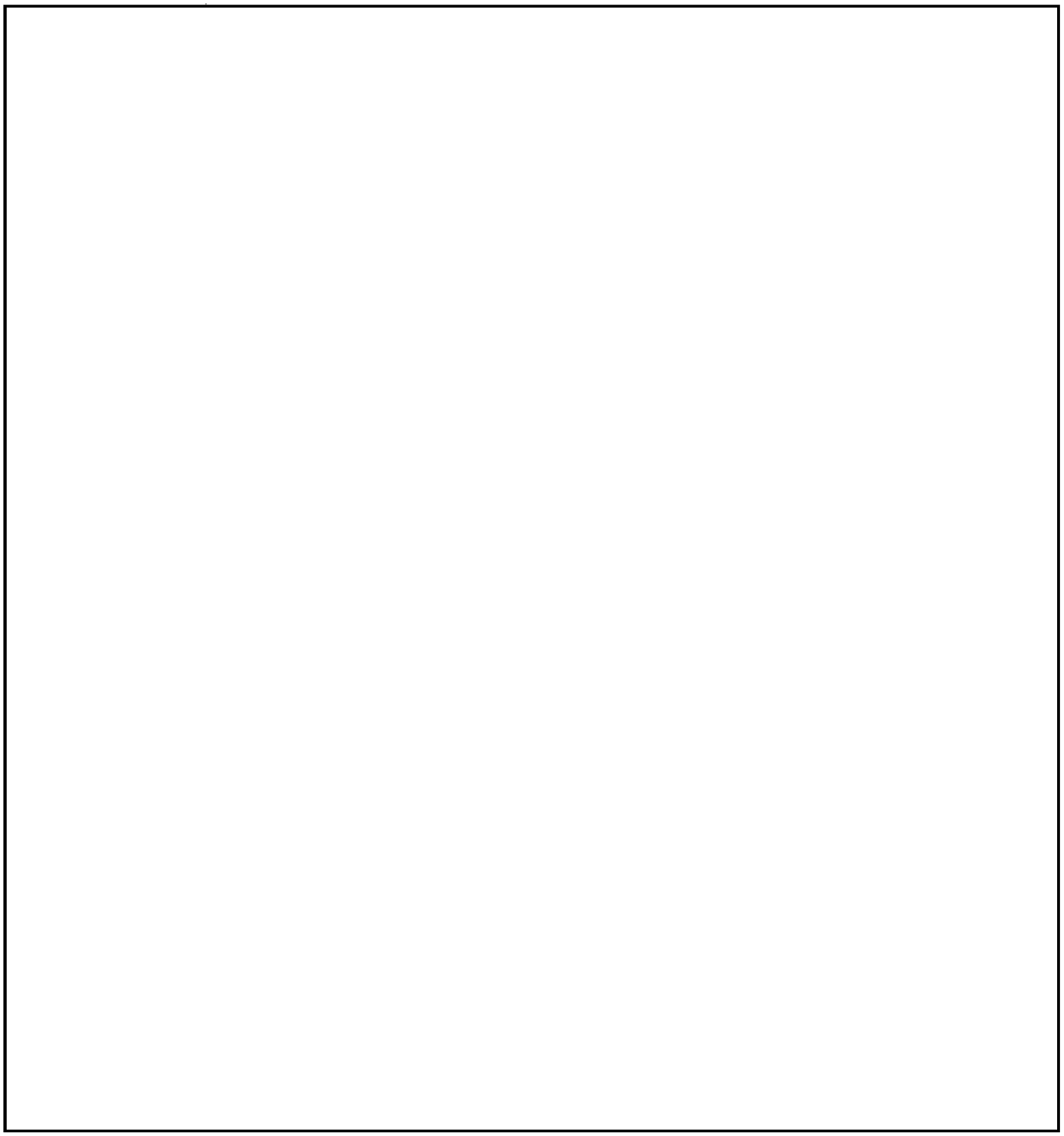
b5



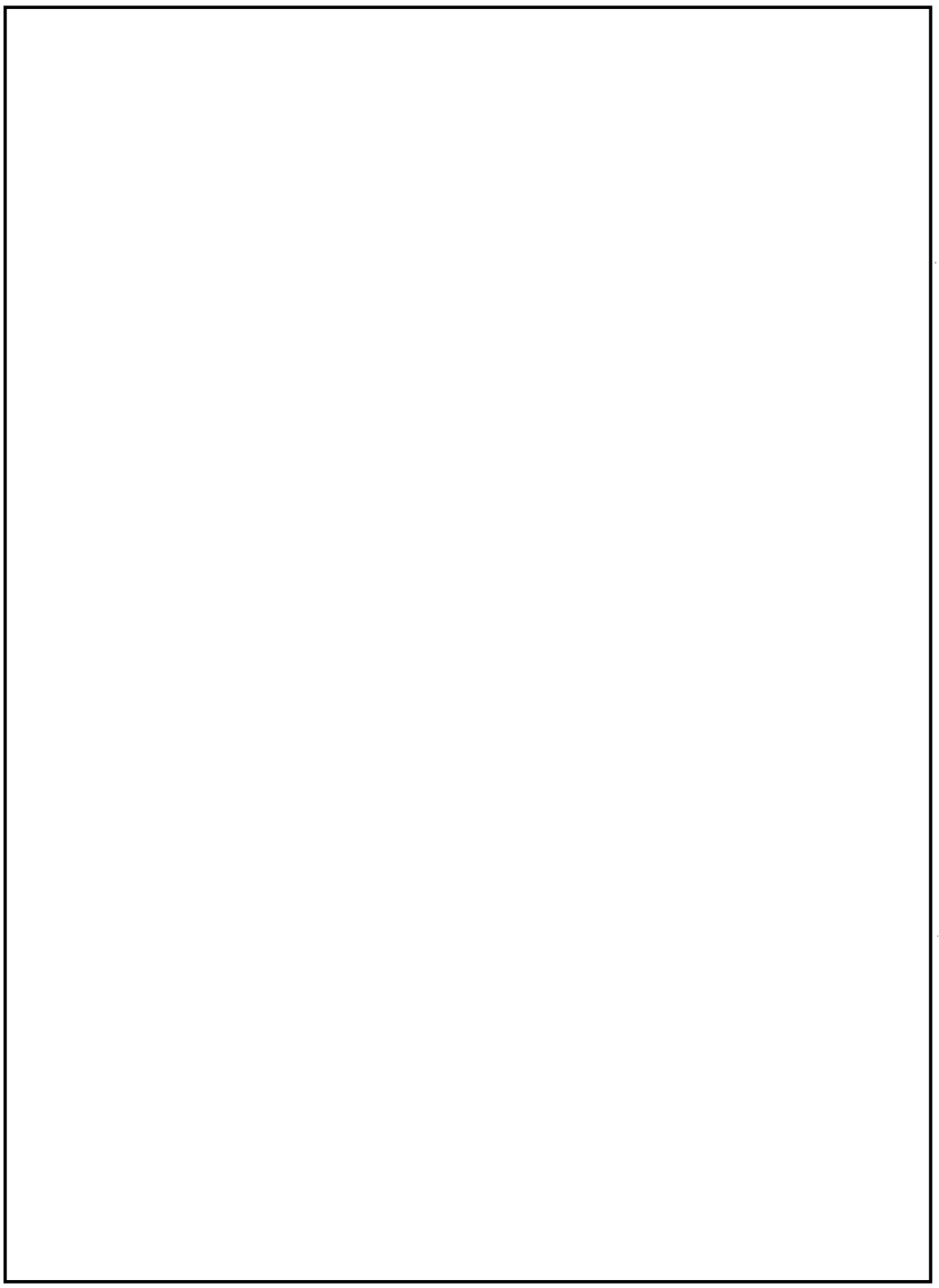




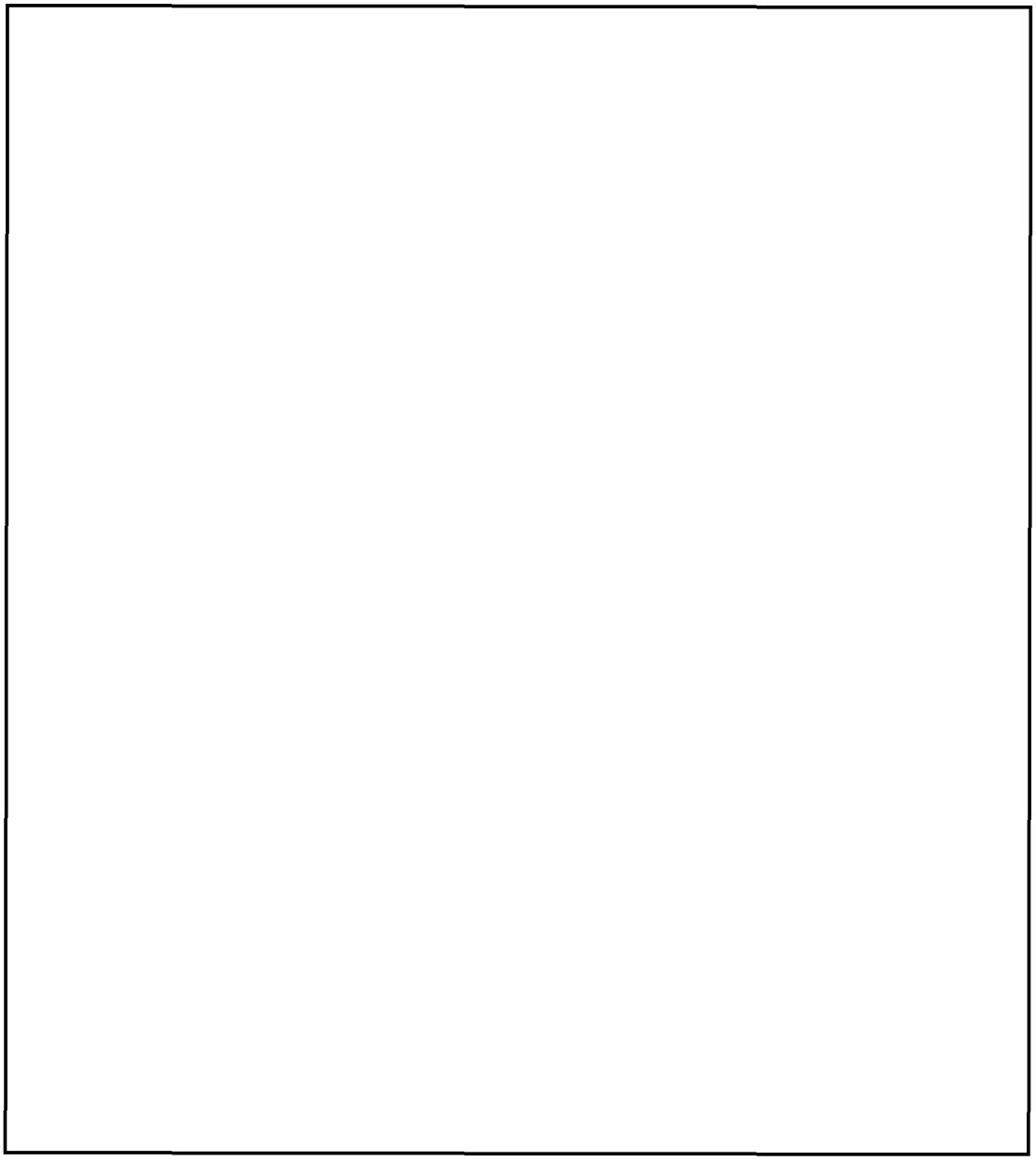
b5



b5



b5



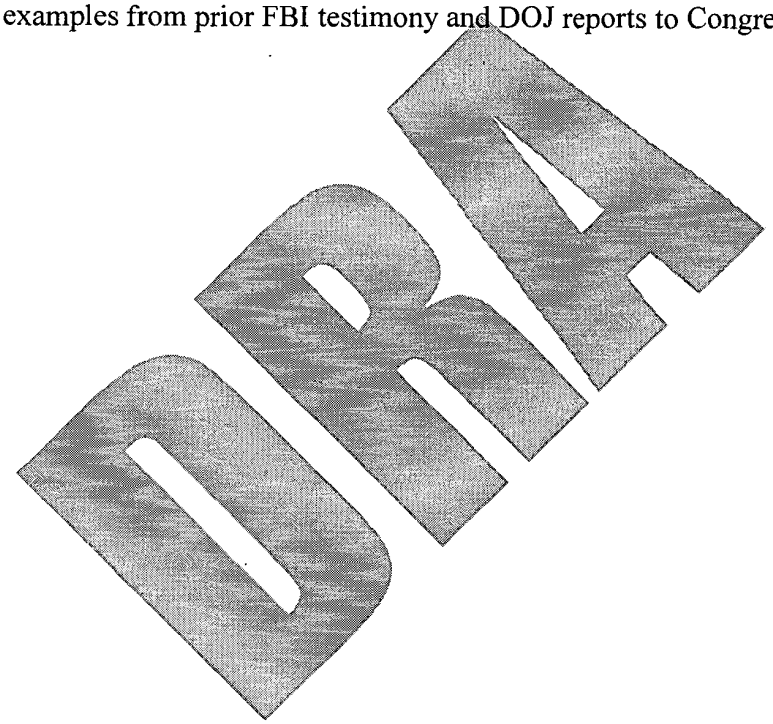
b5

REVISED 3/22/05

FBI
Office of General Counsel
National Security Law Branch

March 22, 2005

The Office of General Counsel has prepared this draft testimony at the request of the Office of Congressional Affairs. This request was received by the author of the draft on March 16, 2005 and the author was required to complete this draft on March 21, 2005. The Office of General Counsel does not have access to the full library of testimony given on this subject and must rely on the Office of Congressional Affairs to ensure that all testimony is consistent with prior testimony given by the Director and other senior FBI officials. The Office of General Counsel has requested that the Counterterrorism Division's International Terrorism Operations Sections I & II provide specific examples for use in this testimony. Such examples have not yet been received by the Office of General Counsel. The author of this draft testimony has therefore relied upon the examples from prior FBI testimony and DOJ reports to Congress.



REVISED 3/22/05

Testimony of Robert S. Mueller, III
Director, Federal Bureau of Investigation
Before the United States Senate
Committee on the Judiciary

April 5, 2005

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to be here today [redacted] b5

[redacted] b5

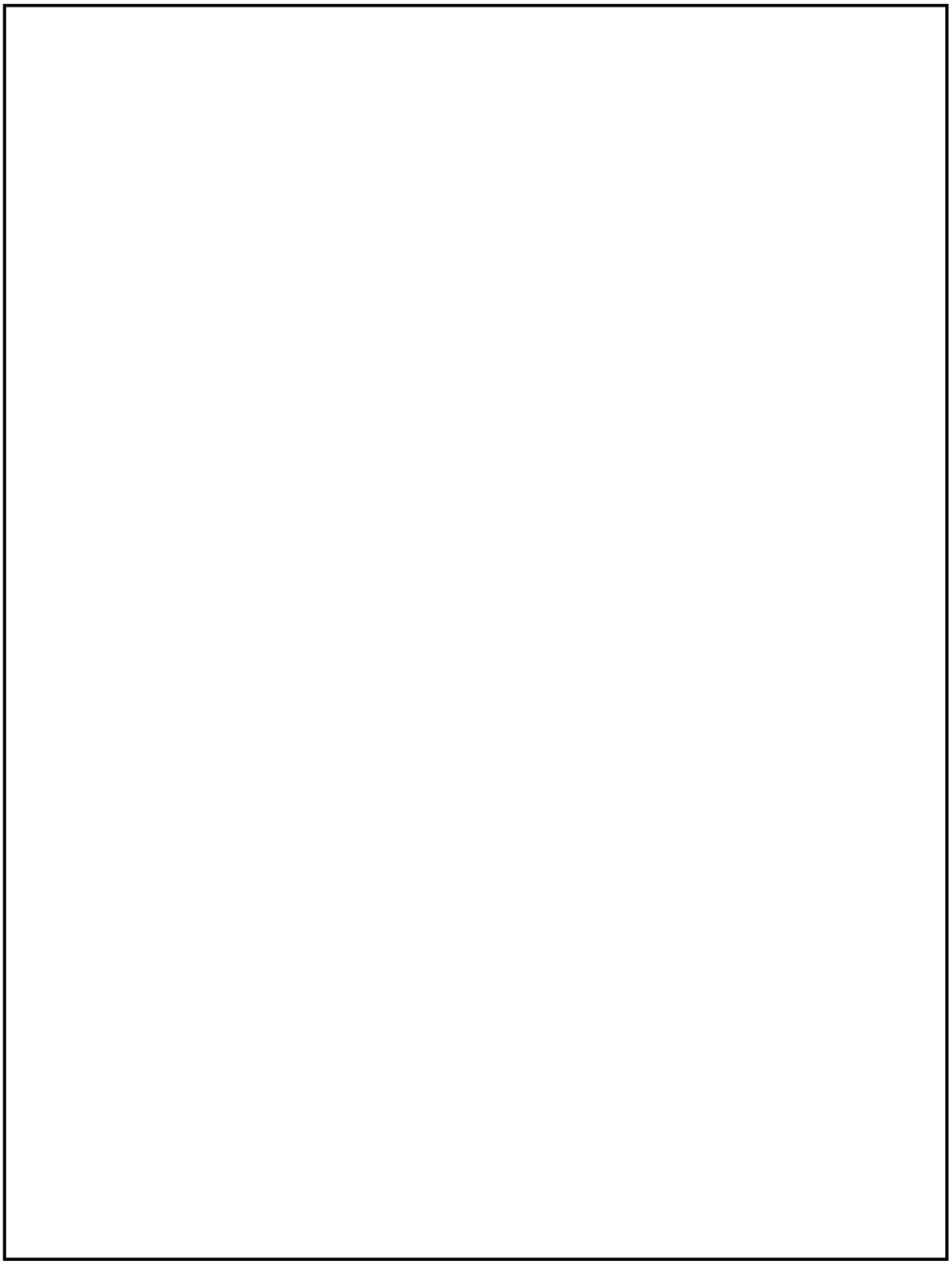
The information sharing provisions are overwhelmingly heralded by our field offices as the most important provisions in the Patriot Act. The new ability to share crucial information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than prior to the Patriot Act.

Specifically, the field offices noted that these provisions enable case agents to involve other agencies in investigations resulting in a style of teamwork that enables more effective and responsive investigations; improves the utilization of resources allowing a better focus on the case; allows for follow-up investigations by other agencies when the criminal subject leaves the U.S.; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the Patriot Act provided for some exchange of information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. The information sharing abilities, due in part to Section 203 of the PATRIOT Act, eliminated that hesitation and allowed agents to work more openly with other government entities resulting in a much stronger team approach. Such an approach is necessary in order to prevent and detect the complex web of terrorist activity. As a result, the field offices report enhanced FBI liaison with State, Local and other Federal agencies, resulting in better relationships.

Even our Legal Attaches (LEGATS) notice improved relationships with foreign intelligence services. If even a portion of the information sharing capabilities are allowed to "sunset" or terminate, then the element of uncertainty that existed in the past would be re-introduced and agents will again hesitate and take precious extra time to seek clarification of the information sharing restrictions prior to sharing information. This hesitation will lead to less teamwork and decreased efficiency. b5

In the aftermath of the September 11th attacks, a reliable intelligence asset identified a naturalized U.S. citizen as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close b5 interaction between the criminal and intelligence case investigators was critical to the successful arrest of the subject before he left the country and the eventual outcome of the case.



b5

Example: In one terrorism case, the only phone that the field office could show was being used by the subject was his associate's phone, and such usage was infrequent. Additionally, the field office did not have sufficient information that this associate was an

agent of a foreign power. Thus, under the previous standard for a FISA pen/trap, the field office may not have succeeded in obtaining the FISA pen/trap order. The new standard established by Section 214 allowed the agents to obtain the pen/trap order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the pen/trap was valuable because it demonstrated the extent to which the subject and his associate were communicating with subjects of other terrorism investigations.

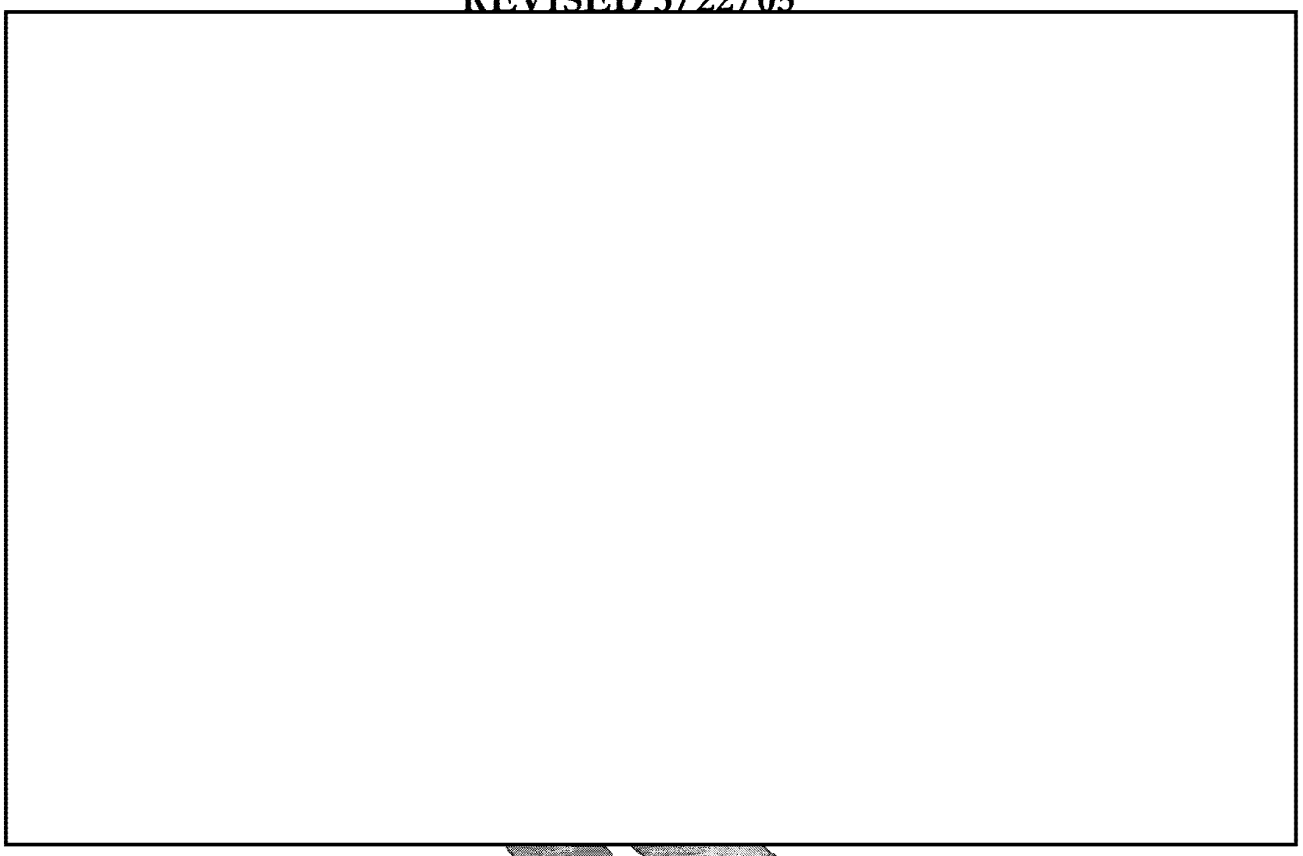
Interception of Computer Trespasser Communications under Section 217

The wiretap statute was amended explicitly to provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a victim of computer hacking could not ask law enforcement to monitor the victim's own computer in an effort to prosecute and stop the intruder. The PATRIOT Act established specific requirements and limitations that must be met before the use of this provision. b5

[redacted] The FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). The group used chat rooms and fraudulent websites, but concealed their activities by using false identities to obtain e-mail accounts. [redacted] The owner of the hacked computer [redacted] was not aware of its use as a conduit for illegal activity. When the victim noticed the unusual activity, he reported the proxy server users to the FBI as trespassers. [redacted] The monitoring provided leads that resulted in the discovery of the true identity of the subject. The subject was indicted in September of 2003. Without the ability to monitor these communications, it would have been unlikely that the FBI could have identified the trespassers.

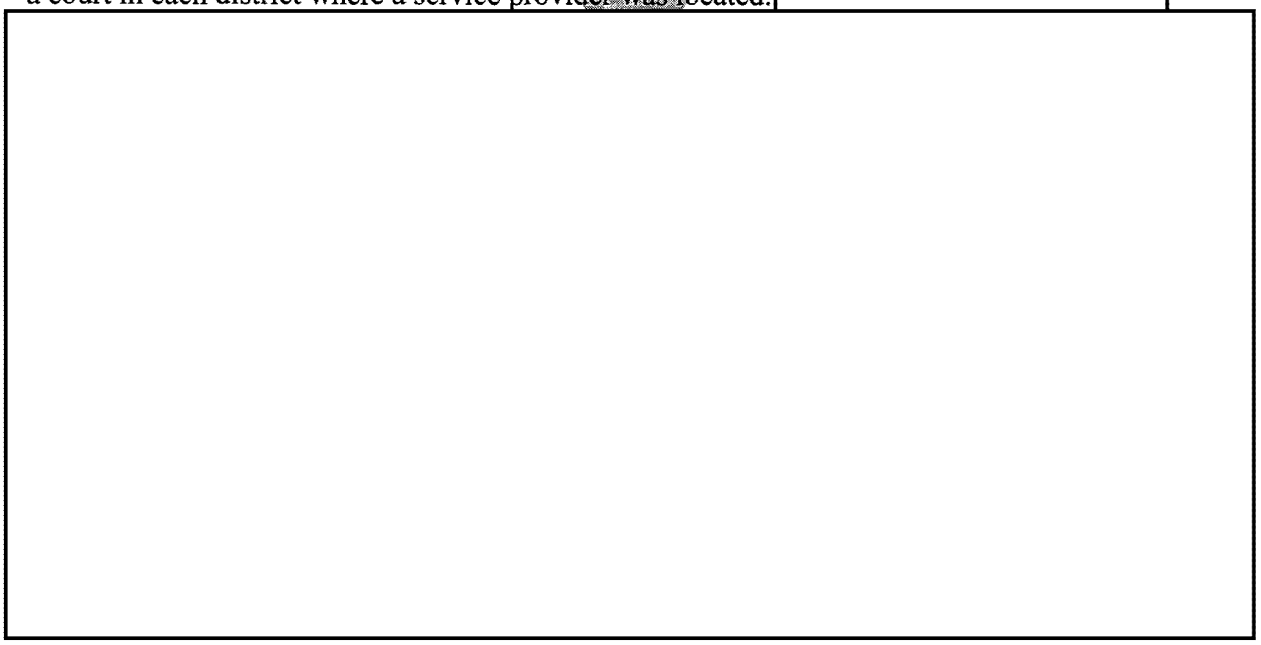
Change in the "Primary Purpose" Standard of FISA under Section 218

Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Moreover, Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant in eliminating "the wall" between criminal and intelligence investigations.



b5

Section 220 of the PATRIOT Act enabled courts to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, such a search warrant had to be issued by a court in each district where a service provider was located.

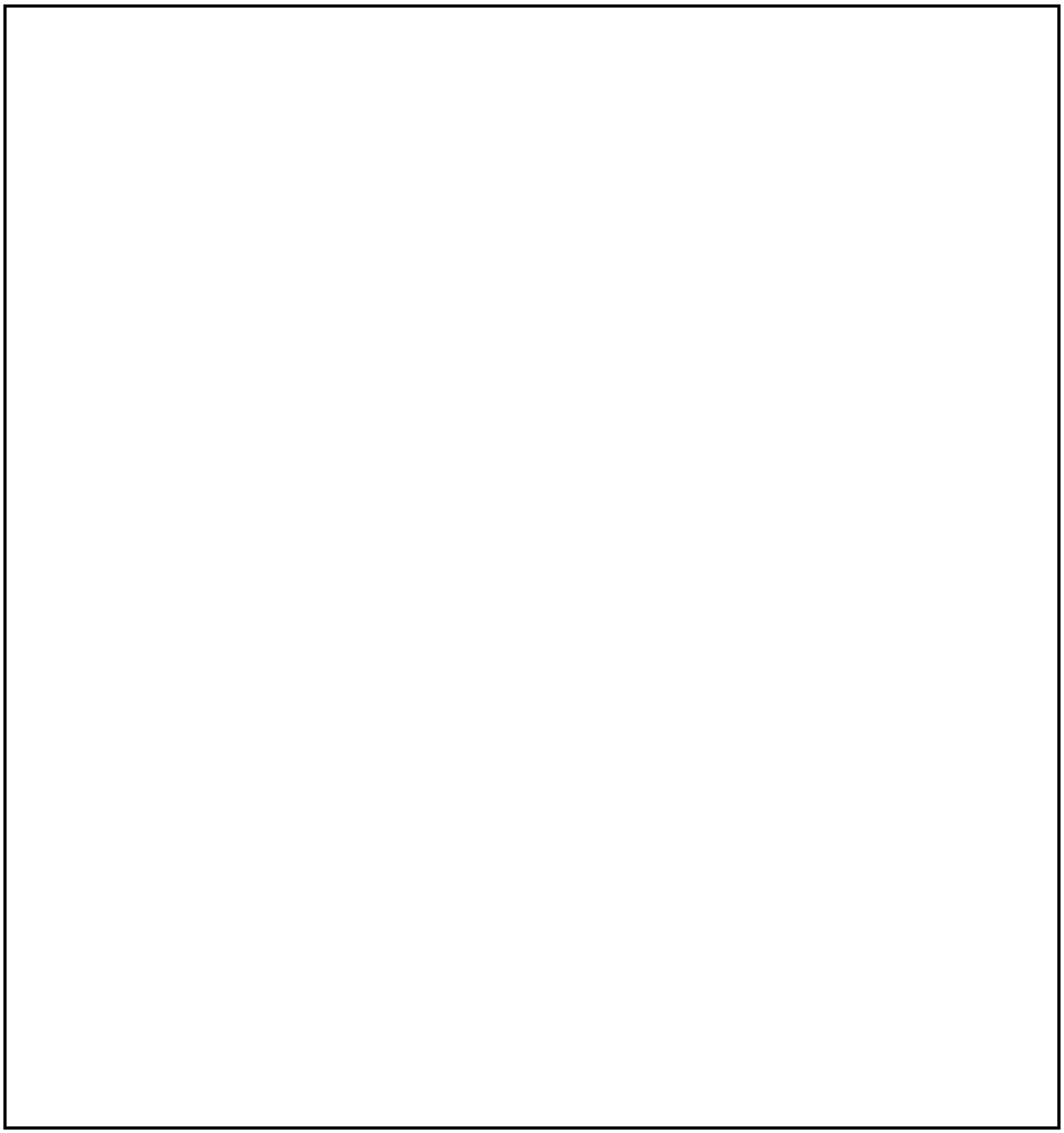


b5

b5

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the PATRIOT Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address two areas in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.



b5

[redacted] b5

Administrative Subpoenas

[redacted]

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

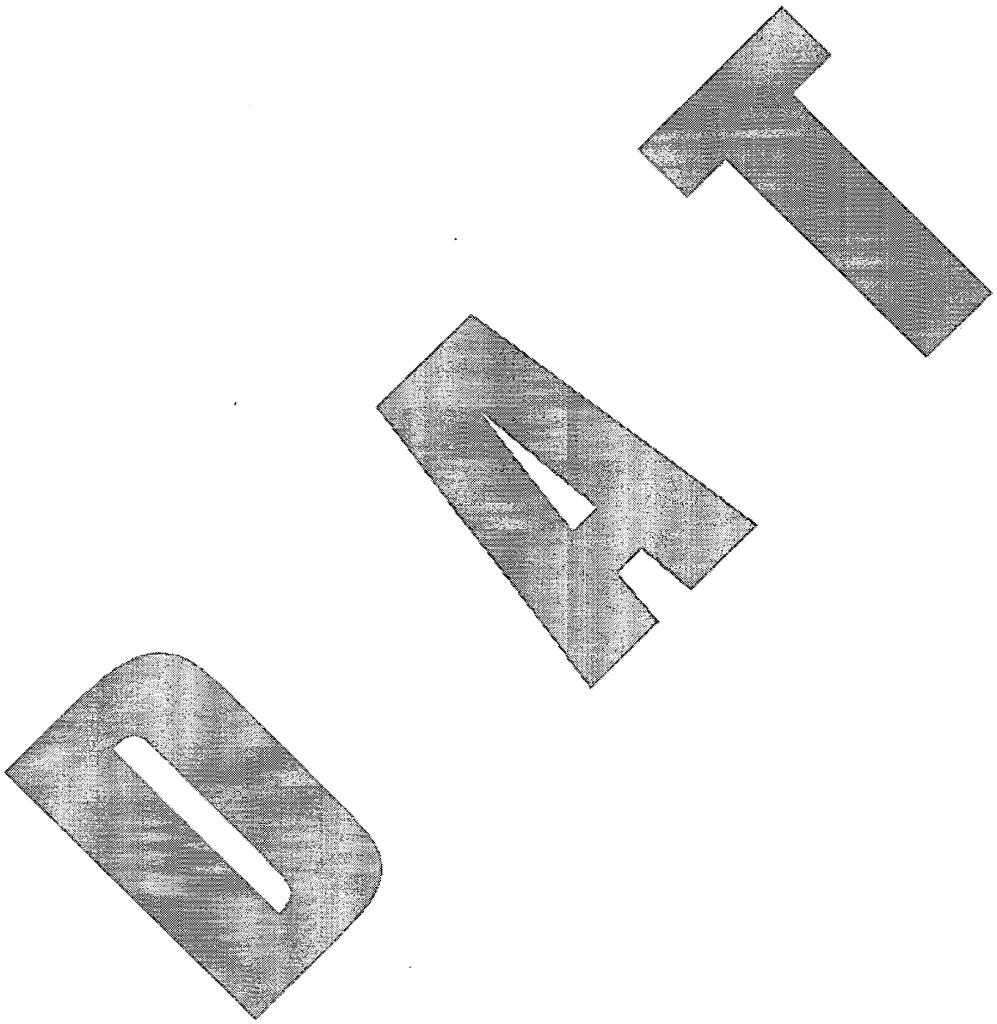
Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and currently there is no enforcement mechanism. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously [redacted] b5

[redacted] The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal could provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the PATRIOT Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes

provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, by granting further modifications to the Foreign Intelligence Surveillance Act and by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today.



REVISED 3/21/05

FBI
Office of General Counsel
National Security Law Branch

March 21, 2005

The Office of General Counsel has prepared this draft testimony at the request of the Office of Congressional Affairs. This request was received by the author of the draft on March 16, 2005 and the author was required to complete this draft on March 21, 2005. The Office of General Counsel does not have access to the full library of testimony given on this subject and must rely on the Office of Congressional Affairs to ensure that all testimony is consistent with prior testimony given by the Director and other senior FBI officials. The Office of General Counsel has requested that the Counterterrorism Division's International Terrorism Operations Sections I & II provide specific examples for use in this testimony. Such examples have not yet been received by the Office of General Counsel. The author of this draft testimony has therefore relied upon the examples from prior FBI testimony and DOJ reports to Congress.

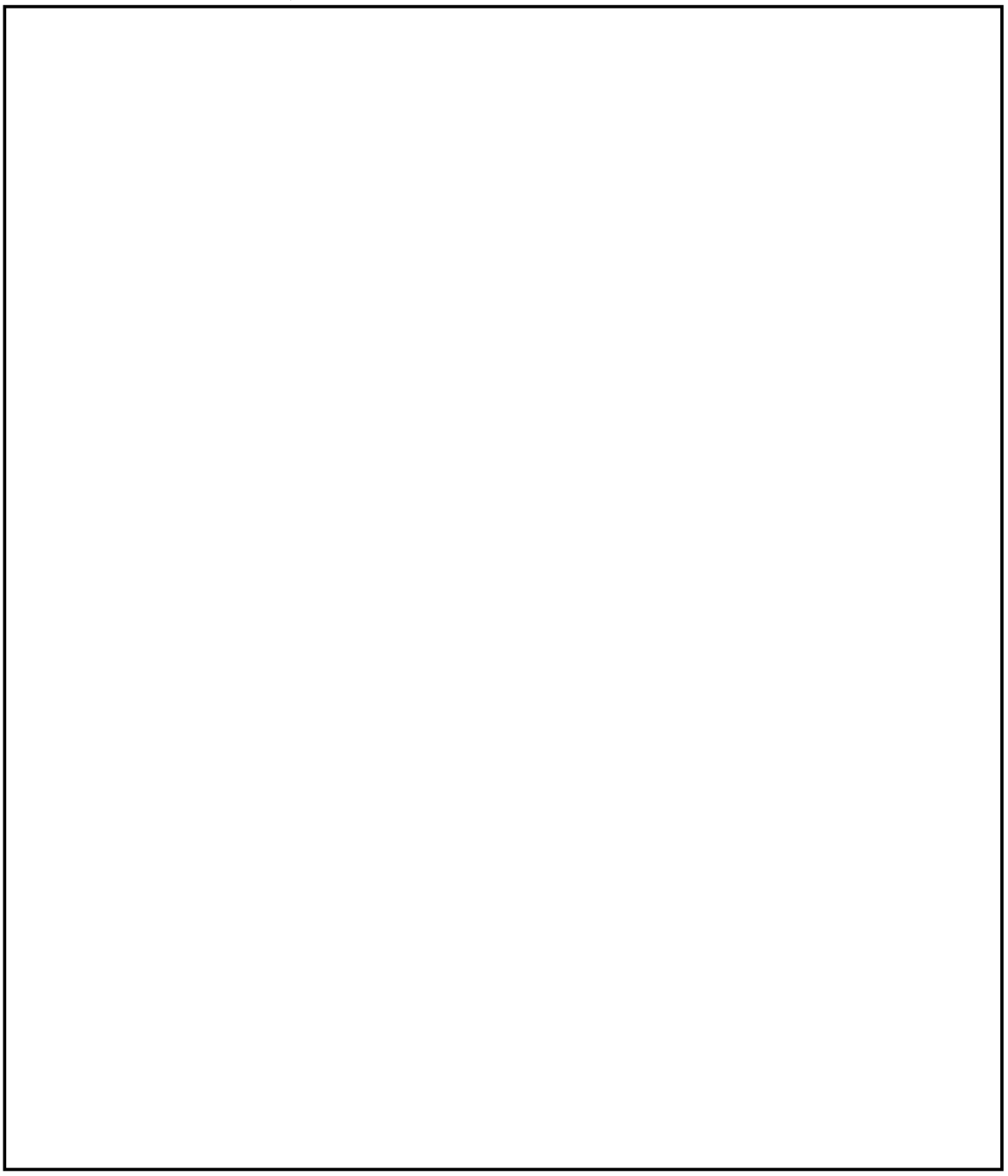
b5

REVISED 3/21/05

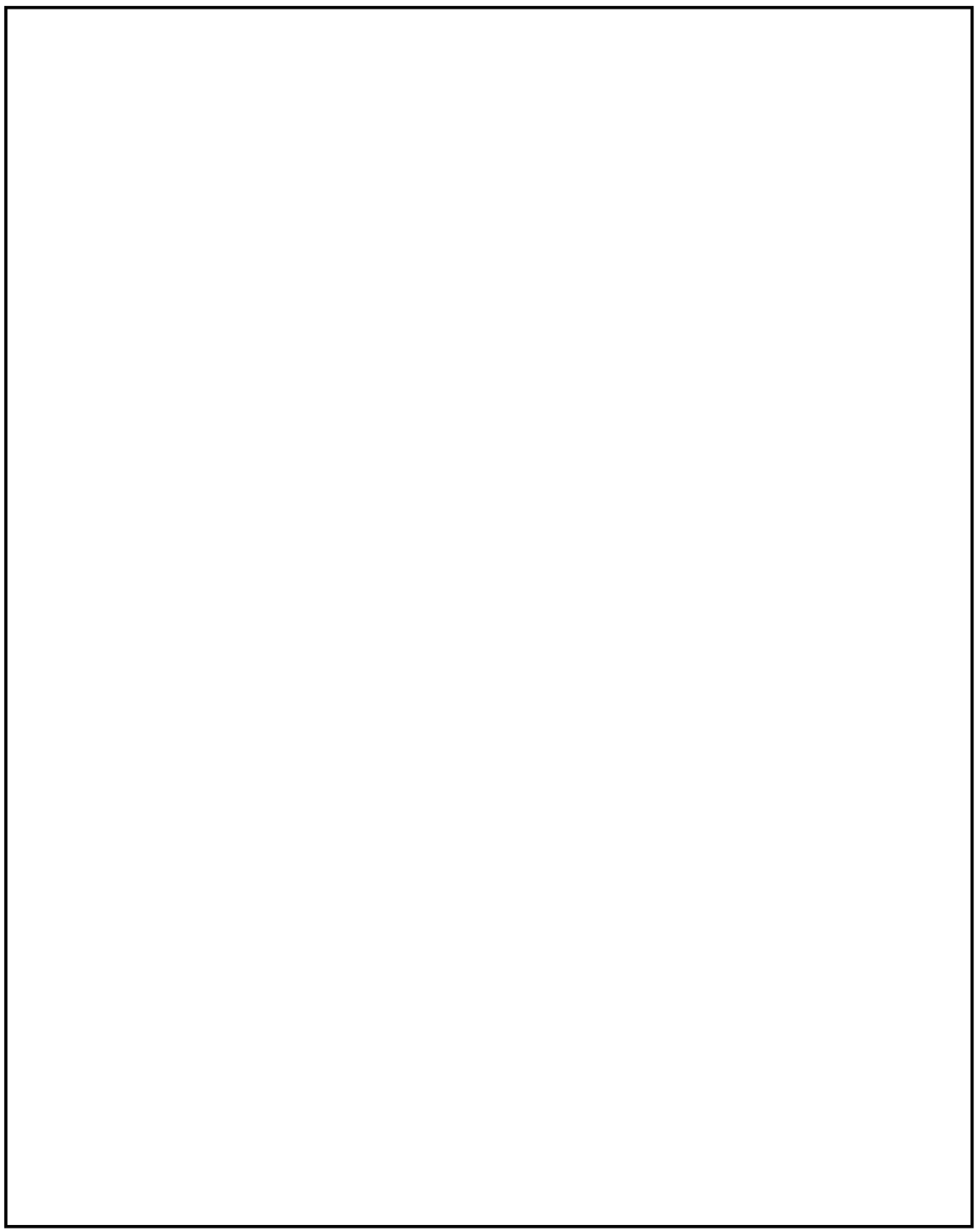
[redacted]

[redacted]

b5



b5



b5

[redacted]

b5

[redacted]

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the PATRIOT Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address two areas in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

[redacted]

b5

[redacted]

b5

Administrative Subpoenas

[redacted]

Planning, funding, supporting and committing acts of terrorism are all federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

b5

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and currently there is no enforcement mechanism. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously this may not be the most effective process to undertake. The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal could provide the recipient the ability to [redacted] quash the subpoena on the same grounds as a grand jury subpoena can be quashed [redacted] b5

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the PATRIOT Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, by granting further modifications to the Foreign Intelligence Surveillance Act and by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today.

From: Caproni, Valerie E. (OGC) (FBI)
Sent: Tuesday, March 29, 2005 2:42 PM
To: [redacted]OCA) (FBI)
Cc: [redacted](OCA) (FBI)
Subject: RE: AG Statement - Patriot Act 215 Language

b6
b7C

UNCLASSIFIED
NON-RECORD

3 comments:

[redacted]

b5

-----Original Message-----
From [redacted](OCA) (FBI)
Sent: Tuesday, March 29, 2005 11:26 AM
To: Caproni, Valerie E. (OGC) (FBI)
Cc: [redacted](OCA) (FBI)
Subject: AG Statement - Patriot Act 215 Language

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b5
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

TREAT AS CLASSIFIED - SECRET
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

Testimony of Robert S. Mueller, III
Director, Federal Bureau of Investigation
Before the United States Senate
Committee on the Judiciary
Sunset Provisions of the USA Patriot Act

April 5, 2004

Good morning Mr. Chairman, Senator Leahy and Members of the Committee. I am pleased to be here today with the Attorney General to talk with you about the ways in which the USA Patriot Act has assisted the FBI with its efforts in the war on terror. For almost three and a half years, the USA Patriot Act has changed the way the FBI operates. Many of our counterterrorism successes are the direct result of the provisions of the Act. As you know, several of these provisions are scheduled to "sunset" at the end of this year. I firmly believe that it is crucial to our national security to keep these provisions intact. Without them, the FBI might well be forced into pre-September 11th practices, requiring us - agents, analysts and our partners - to fight the war on terror with one hand tied behind our back. [redacted] b5

[redacted]

PATRIOT ACT SUNSET PROVISIONS

Section 201 & 202 - Expanded Title III predicates

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing).

Section 201 brought the federal wiretap statute into the 21st century. Prior to its passage, law enforcement was not authorized to conduct electronic surveillance when investigating crimes committed by terrorists, such as chemical weapons offenses, killing U.S. nationals abroad, using weapons of mass destruction, and providing material support to terrorist organizations. Section 201 closed an existing gap in the Title III statute. Now Agents are able to gather information when looking into the full range of terrorism related crimes.

Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III

and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials.

b5

Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials.

The information sharing provisions are overwhelmingly heralded by FBI Field Offices as the most important provisions in the Patriot Act. The ability to share critical information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than prior to the Patriot Act. Specifically, the Field Offices note that these provisions enable case agents to involve other agencies in investigations resulting in a style of teamwork that enables more effective and responsive investigations; improves the utilization of resources allowing a better focus on the case; allows for follow-up investigations by other agencies when the criminal subject leaves the U.S.; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the Patriot Act provided for some exchange of information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. The information sharing abilities, due in part to Section 203, eliminated that hesitation and allow agents to more openly work with other government entities resulting in a much stronger team approach. Such an approach is necessary in order to effectively prevent and detect the complex web of terrorist activity. As a result, the field offices report enhanced FBI liaison with State, Local and other Federal agencies, resulting in better relationships. Even Legats notice improved relationships with intelligence agencies. If even a portion of the information sharing capabilities are allowed to 'sunset' or terminate, then the element of uncertainty is re-introduced and agents will again hesitate and take the time necessary to seek clarification of the information sharing restrictions prior to sharing information. This hesitation will lead to less teamwork and much less efficiency.

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist and foreign intelligence

organizations and acts are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some cases that start out as criminal cases become counterterrorism cases. Some cases that start out as counterintelligence cases become criminal cases. Sometimes the FBI must initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to adequately identify, investigate and address a variety of threats to the United States. The success of these cases is entirely dependent on the free flow of information between the respective investigations, investigators and analysts.

Ongoing criminal investigations of transnational criminal enterprises involved in counterfeiting goods, drug/weapons trafficking, money laundering and other criminal activity depend on close coordination and information sharing with the FBI's Counterterrorism and Counterintelligence Programs, as well as the Intelligence Community, when intelligence is developed which connects these criminal enterprises to terrorism, the material support of terrorism or state sponsored intelligence activity. In one such case, information from a criminal Title III and criminal investigation was passed to Counterterrorism, as well as [redacted] because the subject of the criminal case had previously been targeted by [redacted] agencies. Information sharing permitted each agency to pool their information and resources to investigate the interplay of criminal and foreign intelligence activity. [redacted] b5

[redacted] b5

In one instance, a terrorism case initiated in Minneapolis was subsequently transferred to San Diego and converted to a criminal case. The investigation focused on a group of Pakistan-based individuals who were involved in arms trafficking, the production and distribution of multi-ton quantifies of hashish and heroin, and the discussion of an exchange of a large quantity of drugs for four stinger anti-aircraft missiles to be used by Al Qaeda in Afghanistan. The

operation resulted in the arrest, indictment and subsequent deportation of the subjects from Hong Kong to San Diego to face drug charges and charges of providing material support to Al Qaeda.

[redacted] b5

Criminal enterprises are also frequently involved in, allied with or otherwise rely on smuggling operations. Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens, smuggling anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and smuggling enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities. Current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts, has determined smugglers, as well as illegitimate and quasi-legitimate business operators in the United States, who use the services of illegal aliens. [redacted] b5

In the aftermath of the September 11th attacks, a reliable intelligence asset identified a naturalized U.S. citizen [redacted] as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close interaction between the criminal and intelligence cases was critical to the successful arrest of the subject before he left the country and the eventual outcome of the case. b5

Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

[redacted] b5

[redacted] b5

Section 206 - Roving FISA Surveillance

With this provision, when a FISA target's actions have the effect of thwarting surveillance, such as by rapidly switching cell phones, Internet accounts, or even meeting venues, the Court can issue an order directing as yet unknown cell phone carrier [redacted] b5
(S) [redacted] to effect the authorized electronic surveillance. This allows the FBI to go directly (S) b1
to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order.

Section 206 has been extremely helpful especially in regard to IT and FCI investigations where targets move quickly and often act evasively to avoid detection. Field offices have observed counterintelligence targets change services for hard-line telephones, [redacted] b5
and cell phones numerous times. The roving authority allows them to continuously monitor these targets without interruption. By minimizing the need to return to the court for additional authorizations, it also has allowed agents to more expeditiously conclude investigations [redacted] b1
[redacted]

In one case, a roving FISA on a subject's cellular telephone was approved for the subject of a counterintelligence investigation who, per the usage of tradecraft, is directed to change his cellular phone every four to six months. The roving FISA allows us to continue coverage on all cell phones the subject obtains.

[redacted] b5

Section 207 - Extended Duration for Certain FISAs

Section 207 extends the standard duration for several categories of FISA orders. Before the passage of the USA Patriot Act, FISA orders for electronic surveillance targeted against agents of a foreign power had a maximum duration of ninety days and could be extended in 90-day increments, and orders for a physical search could be issued for no more than forty-five days, unless the target was a foreign power, in which case, the order could be issued for one year. This provision allows orders for physical searches to be issued for certain agents of foreign powers, including United States persons, for ninety days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and agents of foreign powers that are not United States persons. Specifically, initial orders authorizing searches and electronic surveillance can be for periods of 120 days, and renewal orders can be extended for up to one year.

Section 207 has led to reduced paperwork in certain categories of cases. In addition, it has resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under FISA. It has allowed agents to focus their efforts on more significant and complicated terrorism-related cases and to spend more time ensuring that appropriate oversight is given to investigations involving the surveillance of United States persons.

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail.

Section 209 of the USA PATRIOT Act has modernized federal law by enabling investigators to access more quickly suspects' voice-mail by using a search warrant. The speed with which voice-mail is seized and searched can often be critical to an investigation

b5

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury.

Service providers have voluntarily provided information on [redacted] (S) b5 b1 under this provision. Such disclosures often included both e-mail content and associated records. [redacted] This provision has also been utilized to quickly locate kidnaping victims, protect children in child exploitation cases, and to quickly respond to bomb and death threats. [redacted] the Legats have also utilized this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss or serious injury [redacted] b5

In one instance, an FBI Field Division received a bomb threat after hours. After clarifying that the bomb threat was to the local airport and that the FBI had until noon to meet the caller's demands, the FBI JTTF Agents began [redacted] b5 An interview of the subject was conducted and the threat was determined to be non-credible by 11:00 a.m.

In a kidnaping case, a 14 year old girl was abducted. As a result of the FBI's use of this provision, the suspect was quickly identified and interviewed. He admitted to picking up the girl and took agents to the truck stop where he had left her. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours. This is but one example of how essential this provision is for child abduction cases.

Section 214 - FISA Pen/Trap Authority

FISA pen/trap and trace orders [redacted] "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism b5

or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications (i.e. Internet), comparable to the criminal pen/trap provision.

b1
b5

The (S) results from these pen/trap orders often help agents to determine links between the subjects of different terrorism investigations, identify other unknown associates of the subject, discover contacts for potential assets, and develop the subject's personal profile. When pen/trap orders are quickly obtained, they allow agents to more quickly identify the associates tied to the subject of international terrorism investigations than if the agents were required to wait for service providers to respond to subpoenas for toll records, which can take several months. The old standard required more fact gathering to meet the threshold to obtain the pen/trap order, making this technique less effective and sometimes even preventing the use of this technique altogether if the window of opportunity was missed. The FISA pen/trap orders that have been obtained have been used on terrorism and counterintelligence cases, including cases as serious as one where the subject is believed to be attempting to procure nuclear arms.

In one terrorism case, the only phone that the field office could prove was used by the subject was his associate's phone, Additionally, the field office had insufficient information that this associate was an agent of a foreign power. Thus, under the previous standard for a FISA pen/trap, the office may not have succeeded in obtaining the FISA pen/trap order. The standard established by Section 214 allowed the agents to obtain the pen/trap order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the pen/trap was valuable because it demonstrated the extent that the subject and his associate were communicating with subjects of other terrorism investigations.

b5
b1

(S)

In another example, use of this section allowed FISA pen/trap authority based on the fact information was likely to result in foreign intelligence information. This provision allowed the field office to collect data on target lines even when the subject was out of the country and provided valuable intelligence information regarding the subject, the organization and terrorism related matters.

Section 215 - Access to Business Records under FISA

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records (i.e. hotels, motels, car and truck rentals) to include "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

[redacted] b5

Section 217 - Interception of Computer Trespasser Communications

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals that use and trade stolen credit card information). The group utilized [redacted] concealed their identities [redacted] The owner of the hacked computer, [redacted] was not aware [redacted] and considered all individuals [redacted] to be trespassers. [redacted] The monitoring provided leads that resulted in the discovery of the true identity of the subject. The subject was indicted in September of 2003. Without the ability to monitor these communications, it would have been unlikely that the FBI could have identified the trespassers. b5

Section 218 - Change in the "Primary Purpose" Standard of FISA

Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk. b5

As stated above, FBI field offices overwhelmingly herald the information sharing provisions as the most important provisions in the USA Patriot Act. Section 218 is an essential component to these changes. This provision [redacted] prosecutors to be involved in the earliest phases of an international terrorism investigatio[redacted] AUSAs are often co-located with the JTTFs and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks. b5

The ability to have criminal prosecutors involved in the earliest investigative phases of terrorism cases allows counterterrorism investigators to utilize the full selection of both intelligence and criminal investigative tools, enabling them to select and interchange these tools to meet the investigative demands of each particular case. Field offices are now able to use criminal prosecution, or the threat thereof, in furtherance of the intelligence objective to disrupt and dismantle terrorism, towards the ultimate goal of preventing terrorist acts. One field office notes that if 218 were allowed to "sunset," its aggressive and effective investigative approach toward terrorism would be "severely crippled."

[redacted] b5

[redacted] b5

Section 220 - Nationwide Search Warrants for Electronic Evidence

Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warran[redacted] to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703. b5

The FBI routinely relies upon this provision when a search warrant is used to obtain the content of e-mail messages and other related information from Internet service providers (ISPs) in accordance with 18 U.S.C. § 2703. [redacted] (S) b5 b1

Prior to the Patriot Act, if an investigator sought a search warrant to obtain the content of un-opened e-mail from a service provider, the investigator was required to obtain this search warrant from a court in the jurisdiction where the service provider was located. To accomplish this, the case agent would brief an agent and prosecutor located in the ISP's jurisdiction on the facts of the case so that they might appear before the court and obtain the search warrant. This was a time and labor consuming process. Furthermore, because several of the largest ISPs are located in the Northern District of California [redacted] and the Eastern District of Virgini[redacted] hese offices were faced with a substantial workload just to obtain search b5 b5

warrants for other offices.

While the Patriot Act maintained the legal standard that must be met before the search warrant could be issued, that is probable cause, it eliminated the additional bureaucratic paperwork necessary to obtain that warrant in a different jurisdiction than the investigation itself. This eliminated the need to involve additional agents and prosecutors located in the same jurisdiction as the ISP. Therefore, this provision expedites the process and minimizes the labor involved without altering the privacy protection afforded the e-mail and other associated records.

Field offices repeatedly stated that this was very beneficial to quickly obtain information required in the investigation. The information obtained from these search warrants often leads to additional electronic evidence that is easily and quickly lost, therefore minimizing the time required to obtain the initial information from the ISPs is a significant asset to the investigations.

The "Virginia Jihad" case six subjects pled guilty and three were convicted of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. They received sentences ranging from a prison term of four years to life imprisonment. As a part of this case, court orders were issued to Internet Service Providers throughout the country to obtain information related to a vast number of e-mail accounts that resulted in valuable intelligence and criminal evidence used in the successful prosecution. Due to Section 220, all the court orders were issued by the district court where the prosecution occurred making the process much faster and more efficient.

This provision is regularly used in child pornography cases as agents obtain information from ISPs regarding those trading sexually exploitive images of children. This expedites the investigative process and minimizes the number of FBI, U.S. Attorney, and judicial personnel involved in the process freeing them to more aggressively pursue investigative matters.

b5

Section 223 - Civil Liability for Certain Unauthorized Disclosures

Prior to the passage of the Patriot Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this

inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Section 225 - Immunity for Compliance with FISA Wiretap

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISC to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent or a foreign power, such as international terrorists and spies. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers, such as telephone companies [redacted] to carry out such court orders. Prior to the passage of the Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out wiretap and surveillance orders issued by the FISC under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISC without delay. b5

In an FBI Field Office, a case agent was able to convince [redacted] to assist in the installation of technical equipmen[redacted] pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. The target was an espionage subject. [redacted] b5

[redacted]

Section 213 - Delayed Notice Search Warrants

While not scheduled to sunset, the Patriot Act's delayed notice provision, Section 213, has been the subject of criticism and various legislative proposals. The FBI [redacted] believe that Section 213 is an invaluable tool in the war on terror and our efforts to combat serious criminal conduct. It is important to note that delayed notice warrants were not created by the Patriot Act. Rather, the Act simply codified a common law practice recognized by courts across the country and created a uniform nationwide standard for the issuance of those warrants. [redacted] ensures that delayed notice search warrants are evaluated under the same criteria across the nation. Like any other search warrant, a delayed notice search warrant is issued by a federal judge only upon a showing that there is probable cause to believe that the property to be searched for or seized constitutes evidence of a criminal offense. A delayed notice b5

warrant differs from an ordinary search warrant only in that the judge specifically authorizes the law enforcement officers executing the warrant to wait for a limited period of time before notifying the subject of the search that a search had been executed.

Delayed notice search warrants provide a crucial option to law enforcement and can only be requested if one of five narrowly tailored circumstances is present. The FBI has requested this authority in several cases. In most instances, the FBI seeks delayed notice when contemporaneous notice would reasonably be expected to cause serious jeopardy to an ongoing investigation.

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the PATRIOT Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address two areas in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

b5

b5

Administrative Subpoenas

b5

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and currently there is no enforcement mechanism. FISA business record requests require the submission of an

application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously [redacted] b5

[redacted]

The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal could provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the PATRIOT Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, [redacted] b5

[redacted] by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today. I am happy to answer any of your questions.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 4
Page 22 ~ Referral/Direct
Page 23 ~ Referral/Direct
Page 24 ~ Referral/Direct
Page 25 ~ Referral/Direct

#1017326

USA PATRIOT Act
Reauthorization Briefing Book
Valerie E. Caproni
General Counsel
Senate Judiciary Committee

TABLE OF CONTENTS

b6
b7C

	from OIPR, March 30, 2005
TAB 13	Section 215 Access to Business Records and Other Items Under FISA
TAB 14	215 Tweaks
TAB 15	FISA Roving Authority Requests Chart from OIPR, March 30, 2005
TAB 16	Section 206 Roving Surveillance Authority Under FISA

USA PATRIOT Act Provisions Subject to Sunset

Section	Description	Comment
201 (18 USC § 2516(1)(q))	Adds to the predicate offenses for wiretaps : 18 USC § 229 (chemical weapons); § 2332 (crimes of violence against Americans overseas); § 2332a (weapons of mass destruction); § 2332b (multinational terrorism); § 2332d (financial transactions with terrorist countries); § 2339A (supporting terrorists); § 2339B (supporting terrorist organizations)	Applies to Title-III wiretaps
202 (18 USC § 2516(1)(c))	Adds to the predicate offenses for wiretaps : 18 USC § 1030 (computer fraud & abuse)	Applies to Title-III wiretaps
203(b) (18 USC § 2517(6))	Authorizes disclosure of FI, CI and FI information acquired pursuant to Title III to law enforcement, intelligence, protective, immigration, national defense, and national security officials	[redacted]
203(d) (50 USC § 403-5d)	Authorizes disclosure of FI, CI and FI information acquired in a criminal investigation to law enforcement, intelligence, protective, immigration, national defense, and national security officials	b5
204 (18 USC § 2511(2)(f))	Makes clear that the general pen register/trap & trace proscriptions do not bar execution of FISA pen register or trap & trace orders	
206 (50 USC § 1805(c)(2)(B))	"FISA roving surveillance" Authorizes FISA orders to command the assistance of individuals not specifically identified in the order in cases in which the target has taken steps to prevent the identification of specified persons	LE already had this under Title III; [redacted]
207 (50 USC § 1805(e), 1824(d))	Extends duration of FISA orders directed against agents of a foreign power to 120 days and permits extensions at intervals of up to 1 year [up from 90 days (surveillance) & 45 days (searches) for both original orders and extensions]	[redacted] b5
209 (18 USC § 2709; 2510(1),(14))	Makes clear that law enforcement access to voice mail requires only a search warrant	Requirements applicable to Title III wiretaps are more restrictive than search warrants

212 (18 USC § 2702; 2703)	Permits communications service providers to disclose customer records or content of customer communications in an emergency situation involving the immediate danger of serious bodily injury	
214 (50 USC § 1842; 1843)	Authorizes FISA pen register/trap & trace orders with respect to *electronic* communications [e-mail address, URL identification (but not content)] under procedure previously limited to *wire* communications (telephone number of source and addressee); eliminates requirement that the communication either be that of terrorists or spies or related to their criminal activities	
215 (50 USC §§ 1861; 1862)	Authorizes FISA court orders for business records and other tangible items in investigations of international terrorism or espionage (or IAW PL 107-108, §314(a)(6), to obtain foreign intelligence information not concerning a US person)	Most controversial of the sunset provisions; perceived to allow the FBI to raid libraries -- no library has been searched pursuant to this provision. Court order is required (based on "relevance" to an authorized IT or CI investigation
217 (18 USC §§ 2511(2)(i); 2510(21))	Authorizes interception of communications to/from a trespasser within a protected computer	
218 (50 USC §§ 1804(a)(7)(B); 1823(a)(7)(B))	Changes the certification required for a FISA order from "the purpose" to "a significant purpose" to collect FI information; earlier language (which would be revived at sunset) was the one basis for the "wall" between intelligence and criminal investigations	Had a lot to do with demise of "the wall" between intelligence and LE investigations; perhaps the single most productive change to FISA yet.
220 (18 USC §§ 2703; 3127)	Authorizes service anywhere in the world of a court order granting law enforcement access to the content of voice mail and e-mail communications (and/or related records) held by service providers; previously, such orders had to be issued in the place where they were to be executed	

~~SECRET~~

MEMORANDUM

To: General Counsel Valerie Caproni

From: Unit Chief [redacted] b6 b7C

Date: April 1, 2004

SUBJ.: Business Record Requests b1 b3 T50 USC 1861 b6 b7C

§215 REQUESTS APPROVED SINCE JULY 2004

- [redacted] (S)
- [redacted] (S)
- [redacted] (S)
- [redacted] (S)
- [redacted] (S)

(The above list I verified with [redacted] at OIPR. Our branch records show the following business records as having been completed projects, although I did not verify these with OIPR. Please let me know if verification is needed.) b6 b7C

ADDITIONAL §215 REQUESTS

~~SECRET~~

- [redacted] (S)
- [redacted] (S)
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

b1
b3 T50 USC 1861
b6
b7C

(For the above, the NSLB database does not list the type of records requested/obtained. I will obtain for you, if needed.)

PENDING REQUESTS [redacted] (S)

- [redacted] (S)
- [redacted] (S)
- [redacted] (S)
- [redacted] (S)
- [redacted]

b1
b3 T50 USC 1861
b6
b7C

- [redacted] (S)
- [redacted] (S)
- [redacted] (S)
- [redacted] (S)
- [redacted] (S)
- [redacted] (S)

b1
b3 T50 USC 1861
b6
b7C

SECRET//ORCON,NOFORN

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 10-24-2005
CLASSIFIED BY 65179 dmh/elh
REASON: 1.4 (c)
DECLASSIFY ON: 10-24-2030

(S)

(S)

SECRET//ORCON,NOFORN

b1
b2
b3 T50 USC 1861
b6

(S)

b1

b2

b3 T50 USC 1861

b6

O/S [redacted] (S)

(S)

b1

b2

b3 50 USC 1861 18 USC 2517

(S)

b1

b2

b3 T50 USC 1861

b6

(S)

b1
b2
b3 T50 USC 1861
b6

(S)

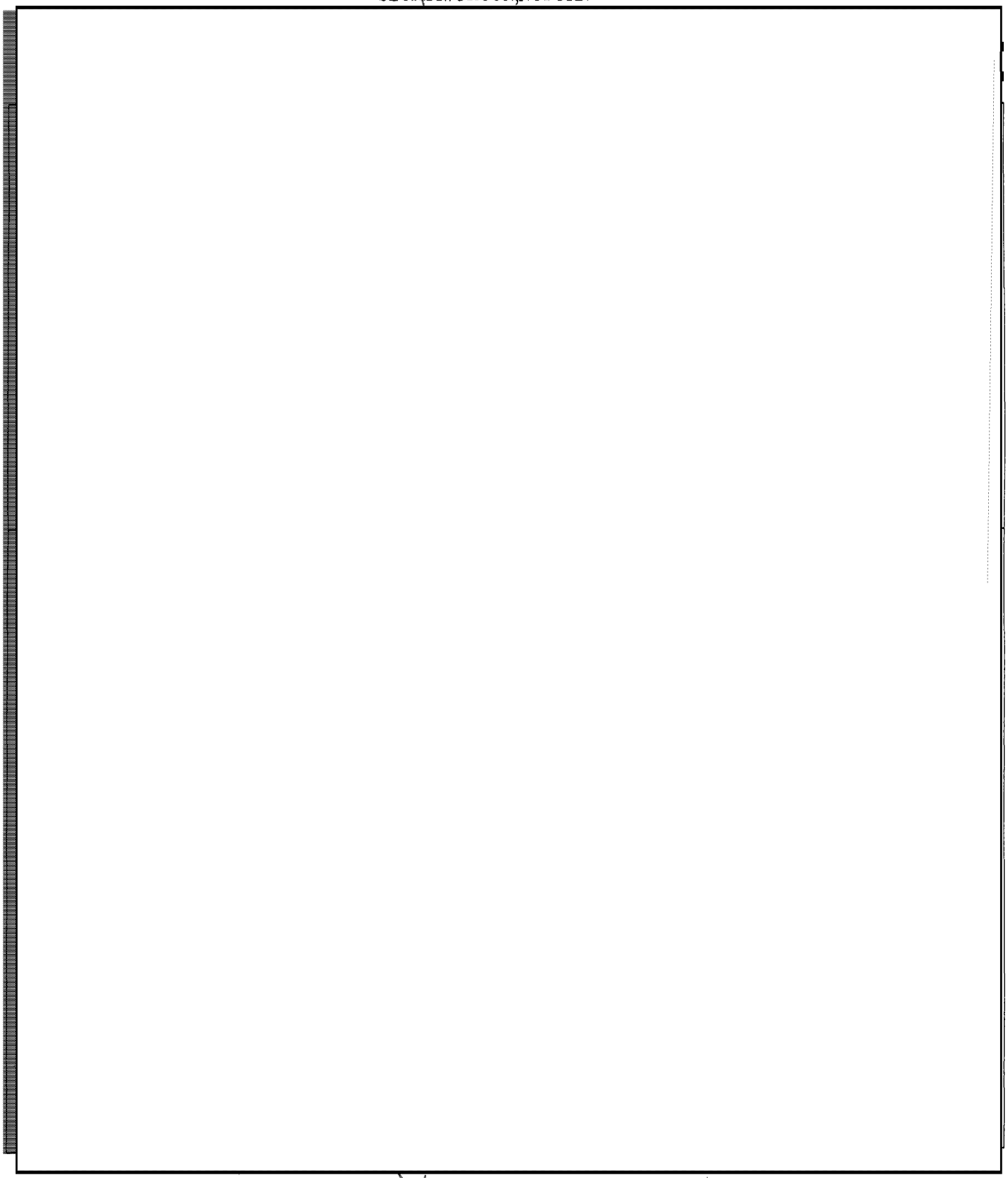
b1

b2

b3 T50 USC 1861

b6

(S)



b1

b2

b3 T50 USC 1861

b6

(S)

b1
b2
b3 T50 USC 1861
b6

(S)

b1

b2

b3 T50 USC 1861

(S)

b1

b2

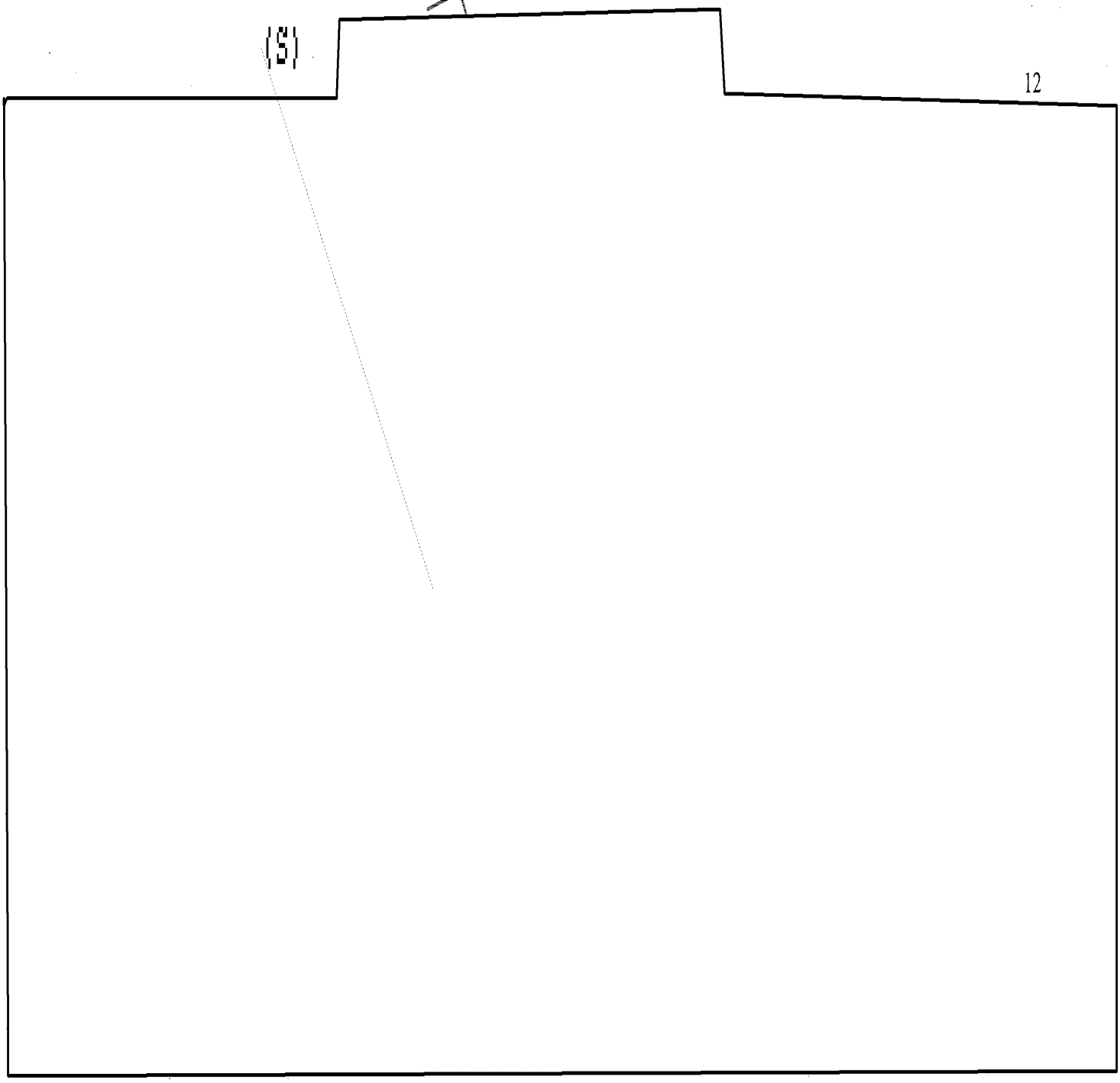
b3 T50 USC 1861

(S)

b1
b2
b3 T50 USC 1861
b6

(S)

12



b1

b2

b3 T50 USC 1861

b6

b7C

Section 215. Access to Business Records and Other Items under FISA

- Section 215 gives the FISA Court the authority in foreign intelligence investigations, such as those involving international terrorism and espionage, to order the production the same kinds of tangible things that prosecutors have always been able to obtain through grand-jury subpoenas in criminal investigations.

- **Before the USA PATRIOT Act**, it was difficult for investigators to obtain court orders for access to business records in connection with foreign intelligence investigations.

- Section 215 improved FISA's original business-records authority in a number of respects:

  - It expanded the **types of entities** that can be compelled to disclose information. Under the old provision, the FBI could obtain records only from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." The new provision contains no such restrictions.

  - It expanded the **types of items** that can be requested. Under the old authority, the FBI could only seek "records." Now, the FBI can seek "any tangible things (including books, records, papers, documents, and other items)."

- Although the FISA Court could now issue a section 215 order to a library so long as a judge determined that the library possessed records relevant to an international terrorism or espionage investigation, **the provision does not single libraries out or even mention them at all**; it simply does not exempt libraries from the range of entities that may be required to produce records.

- The library habits of ordinary Americans are of **no interest** to those conducting terrorism investigations. However, historically terrorists and spies *have* used libraries to plan and carry out activities that threaten our national security. **We should not allow libraries to become safe havens for terrorist or clandestine activities.**

  - For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office who recently was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.

  - In addition, the Justice Department has confirmed that, as recently as the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates.

- Obtaining business records is a long-standing law enforcement tactic. **For years, ordinary grand juries** have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.

- In a recent **criminal** case, a grand jury served a subpoena on a bookseller to obtain records showing that a suspect had purchased a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.

- In the 1997 **Gianni Versace** murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.

- In the 1990 **Zodiac gunman** investigation, a New York grand jury subpoenaed records from a public library in Manhattan. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.

- Section 215 authorized the FISA court to issue **orders similar to grand-jury subpoenas in national-security investigations**. However, it contains a number of safeguards that protect civil liberties, and is actually ***more*** **protective of privacy** than the authorities for ordinary grand-jury subpoenas.

  - A **court must explicitly authorize** the use of section 215 through a **court order**. Agents cannot use this authority unilaterally to compel any entity to turn over its records. **By contrast, a grand jury subpoena is typically issued without any prior judicial review or approval.**

  - Section 215 **expressly protects First Amendment rights**, unlike federal grand-jury subpoenas. It explicitly provides that the FBI cannot conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States."

  - Section 215 has a **narrow scope**. It can only be used (1) "to obtain foreign intelligence information not concerning a United States person"; or (2) "to protect against international terrorism or clandestine intelligence activities." **It cannot be used to investigate ordinary crimes, or even domestic terrorism.** A grand jury can obtain business records in investigations of *any* federal crime.

- Section 215 orders are also subject to the **same burden of proof as are grand-jury subpoenas**; investigators must meet a standard of relevance.

- Section 215 provides for **congressional oversight**. Every six months, the Attorney General must "fully inform" Congress on how it has been implemented. To date, the Justice Department has provided Congress with six reports regarding its use of section 215.

- **Allowing section 215 to expire would make it much harder for investigators to obtain critical evidence in international terrorism and espionage investigations.**

POSSIBLE QUESTIONS:

Isn't it true that under section 215 of the USA PATRIOT Act, the FISA court is just a rubberstamp because the judge must issue an order requiring the production of records if he or she receives an application from the Department asserting that it is seeking the records in connection with a foreign intelligence investigation, or an investigation to protect against international terrorism or clandestine intelligence activities?

- This description of section 215 is **categorically false.**

- Pursuant to section 215, a judge "shall" issue an order "approving the release of records **if the judge finds that the application meets the requirements of this section.**" 50 U.S.C. § 1861(c)(1) (emphasis added).

- As a result, before issuing an order requiring the production of any records under section 215, a federal judge must find that the requested records are sought for (and thus relevant to) "an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2).

- In addition, a federal judge must find that the investigation is not being conducted of a United States person solely on the basis of activities protected by the First Amendment. 50 U.S.C. § 1861(a)(2)(b).

- Moreover, the United States has stated in litigation that recipients of orders for the production of records under section 215 may challenge the legality of those orders in the FISA Court.

Isn't it true that section 215 orders, unlike grand-jury subpoenas, are not governed by a relevance standard?

- **Section 215 orders are subject to the same relevance standard as are grand-jury subpoenas.**

- **Just as grand-jury subpoenas may be issued to obtain records that are relevant to a criminal investigation, the FISA Court may issue orders requiring the production of records under section 215 that are relevant to an authorized international terrorism or espionage investigation.**

- Some critics have complained that section 215 does not contain a "relevance" standard because **the word "relevance' is not specifically mentioned in the provision itself.**

- Section 215, however, states that the FISA Court may only enter an order requiring the production of records if such records are "**sought for** an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1862(a).

- **This is the equivalent of a relevance standard because if records are irrelevant to an investigation, then they are not being "sought for" that investigation.**

Isn't it true that section 215 explicitly forbids establishments such as libraries from telling their patrons that the government has requested their records? Why shouldn't libraries be able to tell their patrons when the government has requested their records?

- **The provision forbids the recipient of a section 215 order from disclosing to others that the government has requested the production of documents pursuant to section 215.**
    - Section 215, however, contains an explicit exception allowing the recipient of a section 215 order to inform those whose assistance is needed to produce the requested records.
    - The Department also takes the position that section 215 also contains an **implicit exception to the nondisclosure requirement** allowing the recipient of a section 215 order to **inform his or her attorney** of the request for the production of records.
- Such a nondisclosure requirement, however, is standard operating procedure for the conduct of surveillance in sensitive international terrorism or espionage investigations.
- **It is critical that terrorists are not tipped off prematurely about intelligence investigations. Otherwise, their conspirators may flee and key information may be destroyed before the government's investigation has been completed.**
    - As the U.S. Senate concluded when adopting the Foreign Intelligence Surveillance Act: "By its very nature, foreign intelligence surveillance must be conducted in secret."
    - Furthermore, were information identifying the targets of international terrorism and espionage investigations revealed, according to the D.C. Circuit, such disclosures would "inform terrorists of both the substantive and geographic focus of the investigation[,] . . . would inform terrorists which of their members were compromised by the investigation, and which were not[,] . . . **could allow terrorists to better evade the ongoing investigation and more easily formulate or revise counter-efforts** . . . [and] **be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation**." *Center for National Security Studies v. U.S. Department of Justice*, 331 F.3d 918, 928-29 (D.C. Cir. 2003).

While the Department has claimed that section 215 of the USA PATRIOT Act is a vital tool in the war against terrorism, the Department stated in the fall of 2003 that it had yet to use this new authority. If section 215 is such an important provision, then why was it not utilized in its first two years of existence?

- **The fact that an authority may be used infrequently does not denigrate its importance.**

- To the contrary, it is important that the authority exists for situations in which a section 215 order could be critical to the success of an investigation.
    - Just as prosecutors need to obtain relevant records through grand-jury subpoenas in criminal investigations, so, too, do investigators in national-security investigations sometimes need to obtain relevant records.
- **Just as a police officer knows that his firearm may be invaluable in preventing crime, even if he cannot predict when he might need to draw it from his holster, section 215 provides investigators an authority they may find crucial to stop a terrorist plot.**
- **The fact that the Department has used this authority in a judicious manner should not be used as an argument for repealing the provision altogether.**

By restoring the requirement of "specific and articulable facts" that the records sought under FISA pertain to a terrorist, spy or other foreign agent, which merely requires some individual suspicion, wouldn't the SAFE Act greatly limit the danger that section 215 could be misused to secretly obtain the private records of innocent people?

- The SAFE Act would require the FISA Court, before issuing an order for the production of records under section 215, to find that there are "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."
- The SAFE Act would therefore deny terrorism investigators access to crucial intelligence information by raising the standard under which the FISA court can order the production of **business records** and other tangible things.
    - Section 215 orders are currently governed by the same relevance standard that is currently used with respect to grand-jury subpoenas.
    - By imposing a "specific and articulable facts" standard for obtaining business records in a FISA investigation, which is much higher than the simple relevance standard for obtaining a grand-jury subpoena that is also currently used under section 215, the SAFE Act would make it much more difficult to investigate terrorists and spies than to investigate drug dealers or bank robbers.
    - Investigators, for example, would be denied access to records that are indisputably relevant to an international terrorism investigation simply because the records do not specifically pertain to the suspected terrorist.
- Section 215 already contains sufficient safeguards to guarantee that it is not misused to obtain the private records of innocent people, and it is actually ***more*** **protective of privacy** than the authorities for ordinary grand-jury subpoenas.

- A **court must explicitly authorize** the use of section 215 through a **court order**. Agents cannot use this authority unilaterally to compel any entity to turn over its records. **By contrast, a grand-jury subpoena is typically issued without any prior judicial review or approval.**

- Section 215 **expressly protects First Amendment rights**, unlike federal grand-jury subpoenas. It explicitly provides that the FBI cannot conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States."

- Section 215 has a **narrow scope**. It can only be used (1) "to obtain foreign intelligence information not concerning a United States person"; or (2) "to protect against international terrorism or clandestine intelligence activities." **It cannot be used to investigate ordinary crimes, or even domestic terrorism.** A grand jury can obtain business records in investigations of *any* federal crime.

- Section 215 provides for **congressional oversight**. Every six months, the Attorney General must "fully inform" Congress on how it has been implemented. No similar oversight exists with respect to grand-jury subpoenas.

(S)

(S)

b1

b2

b3 T50 USC 1805

(S)

(S)

b1

b2

b3 50 USC 1805

(S)

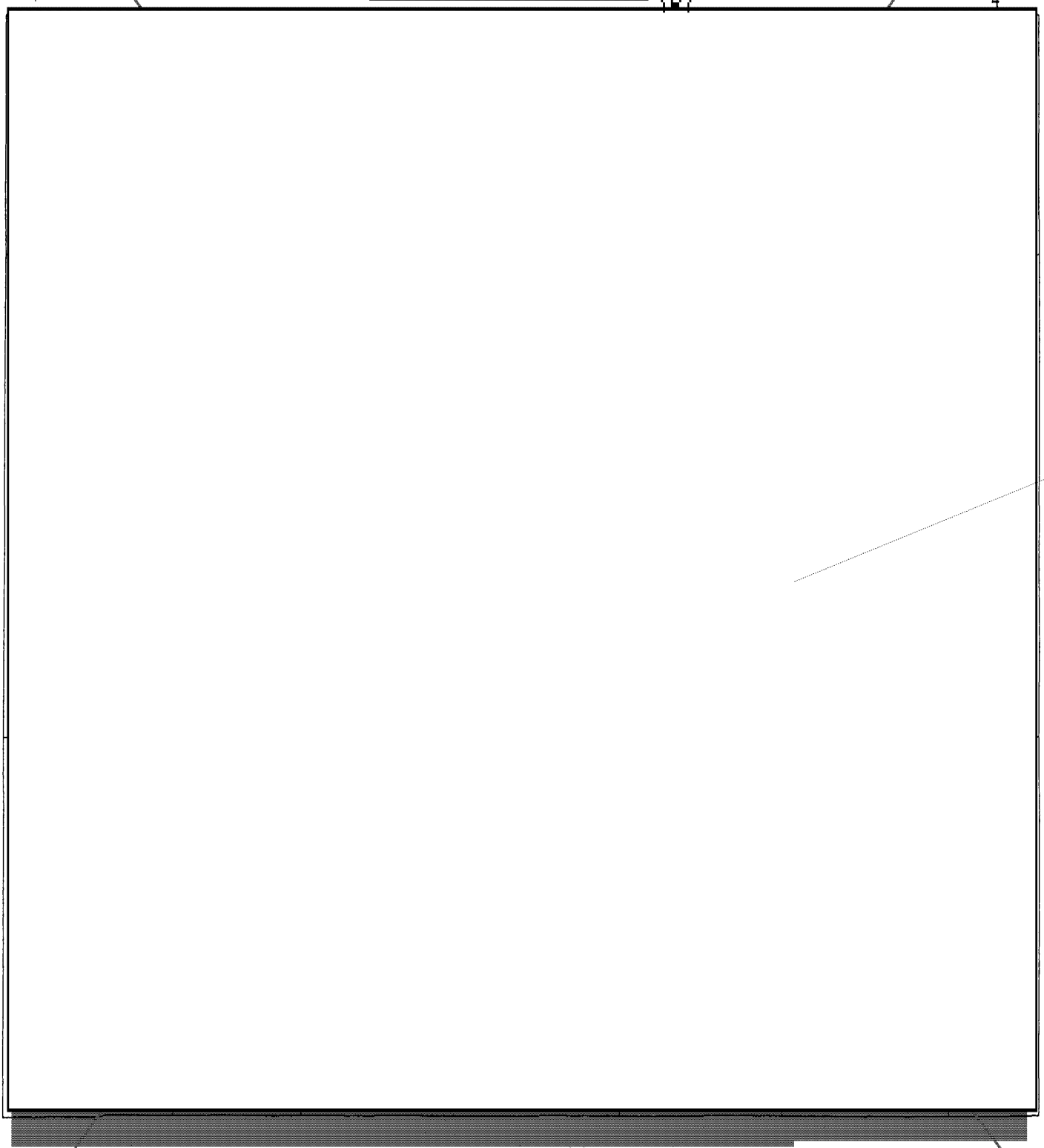
(S)

b1

b2

(S)

4



(S)

b1

b2

b3 T50 USC 1805

(S)

(S)

b1

b2

b3 T50 USC 1805

(S)

(S)

b1

b2

b3 T50 USC 1805

b6

(S)

7

(S)

b1

b2

(S)

(S)

b1

b2

b3 T50 USC 1805

b6

b7C

Section 206. Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978 ("FISA")

- Section 206 allows the FISA court to authorize "roving" surveillance of a terrorist or spy when it finds that the target's actions may thwart the identification of those specific individuals or companies, such as communications providers, whose assistance may be needed to carry out the surveillance.

- A "roving" wiretap order attaches to a particular target rather than a particular phone or other communications facility.

- **Before the USA PATRIOT Act**, the use of roving wiretaps was not available under FISA.

  - Therefore, each time a suspect changed communication providers, investigators had to return to the FISA court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap.

  - **International terrorists and foreign intelligence officers, however, are trained to thwart surveillance** by changing communications facilities just prior to important meetings or communications.

  - As a result, without roving wiretaps, investigators could be left two steps behind sophisticated terrorists.

- **For years, law enforcement has been able to use roving wiretaps to investigate ordinary crimes**, including **drug offenses** and **racketeering**. The authority to use roving wiretaps in traditional criminal cases has existed since 1986.

- Section 206 **simply authorized the same techniques** used to investigate ordinary crimes to be used **in national-security investigations**. This provision has put investigators in a better position to counter the actions of spies and terrorists who are trained to thwart surveillance.

- Section 206 contains a number of **privacy safeguards**.

  - Significantly, section 206 did not change the requirement that the target of roving surveillance must be identified or described in the order.

  - Therefore, section 206 is **always connected to a particular target** of surveillance. [redacted] FISA nonetheless requires the government to provide "a description of the target of the electronic surveillance" to the FISA Court prior to obtaining a roving surveillance order. b2 b7E

  - Section 206 did not alter the requirement that before approving a roving surveillance order, the **FISA Court must find that there is probable cause** to believe the target of the surveillance is either a **foreign power or an agent of a foreign power, such as a terrorist or spy**.

- Roving surveillance under section 206 can be ordered only after the FISA Court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance.

- Moreover, section 206 **in no way altered the rigid FISA minimization procedures that limit the acquisition, retention, and dissemination** by the government of information or communications involving United States persons.

- A number of federal courts – including the Second, Fifth, and Ninth Circuits – have squarely ruled that "**roving" wiretaps are perfectly consistent with the Fourth Amendment**. No court of appeals has reached a contrary conclusion.

- **If section 206 were allowed to expire, investigators would once again often struggle to catch up to sophisticated terrorists and spies trained to take steps such as constantly changing cell phones in order to avoid surveillance.**

POSSIBLE QUESTION:

Because wiretaps are the most intrusive form of surveillance known to the law, is it asking too much to require the government, when it seeks a surveillance order than can jump from telephone to telephone, [redacted]

- FISA currently requires an order approving electronic surveillance to specify, among other things: (1) **the identity, if known, or a description of the target of the electronic surveillance**; and (2) **the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known.**

- Many civil liberties advocates have therefore complained that "roving" wiretaps under FISA **may be used to violate the privacy of innocent Americans** because:

  - FISA allows for the issuance of surveillance orders that **neither specify the locations** that will be placed under surveillance [redacted] and

  - FISA does not contain any requirement that "roving" surveillance may be conducted [redacted] at a particular location is ascertained by the government.

b2
b7E

- The SAFE Act seeks to correct these purported deficiencies in FISA by requiring that:

  - An electronic surveillance order under FISA specify either: [redacted] or (2) the location of each of the facilities or places at which surveillance will be directed; and

- Proponents of the SAFE Act have claimed that this provision would simply impose the same requirement on FISA "roving" wiretap orders as are currently placed on "roving" wiretap orders issued in criminal investigations.

- **This argument, however, is incorrect.**

  - **The specific "ascertainment" requirement** contained in the criminal wiretap statute **applies to the interception of oral communications**, such as through bugging, **and not to the interception of wire or electronic communications**, such as telephone calls.

  - This provision of the criminal wiretap statute states that the interception of an oral communication "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." *See* 18 U.S.C. § 2518(12).

  - With respect to the interception of wire or electronic communications, the criminal wiretap statute imposes a more lenient standard, requiring that surveillance can be conducted "only for such time as it is reasonable to presume that [target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted." *See* 18 U.S.C. § 2518(11)(b)(iv).

- **Congress should not impose restrictions that make it more difficult for investigators to conduct roving wiretaps directed against international terrorists than it is to conduct such wiretaps against drug dealers and those participating in organized crime.**

- **The Department believes that FISA already contains sufficient safeguards to ensure that the government does not intrude on the privacy of innocent Americans.**

  - The target of roving surveillance must be identified or described in the order of the FISA Court. A roving wiretap order is therefore [redacted] of surveillance. b2 b7E

  - The **FISA Court must find that there is probable cause** to believe the particular target of the surveillance is either a **foreign power or an agent of a foreign power, such as a terrorist or spy**.

  - Roving surveillance can be ordered only after the FISA court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance.

  - **FISA requires the use of robust minimization procedures that limit the acquisition, retention, and dissemination** by the government of information or communications involving United States persons.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 20
Page 314 ~ Duplicate
Page 315 ~ Duplicate
Page 316 ~ Duplicate
Page 317 ~ Duplicate
Page 318 ~ Duplicate
Page 319 ~ Duplicate
Page 320 ~ Duplicate
Page 321 ~ Duplicate
Page 322 ~ Duplicate
Page 323 ~ Duplicate
Page 324 ~ Duplicate
Page 325 ~ Duplicate
Page 326 ~ Duplicate
Page 327 ~ Duplicate
Page 328 ~ Duplicate
Page 329 ~ Duplicate
Page 330 ~ Duplicate
Page 331 ~ Duplicate
Page 332 ~ Duplicate
Page 333 ~ Duplicate

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted](OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To: [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted](OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

[redacted] and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcmte on Terrorism and is meant to:
1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments to [redacted] ext. [redacted] by **9:00 am, Tuesday, 2/22/05**.

b2
b6
b7C

Thanks for your assistance.

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

UNCLASSIFIED

~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Monday, March 28, 2005 4:45 PM b7C
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Roving Authority

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie:

FYI. Just closing the loop to keep you informed. Valerie wanted to know the number of Roving FISAs done to date.

[redacted] b6 b7C

DATE: 08-22-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-22-2030

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

AAG

-----Original Message-----
From: [redacted] (OGC) (OGA)
Sent: Monday, March 28, 2005 4:03 PM
To [redacted] (OGC) (FBI)
Cc [redacted] (OGC) (FBI); [redacted] (OGC) (FBI) b6
Subject: RE: Roving Authority b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I just answered a similar question via an email from Valerie. The number of Section 206 orders since the Patriot Act's signing to date is [redacted] Does that give you what you need? Let me know if not, [redacted] b1 b6 b7C

(S)

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, March 28, 2005 10:10 AM
To: [redacted] (OGC) (OGA)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI) b6
Subject: Roving Authority b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I am writing to follow up on a phone conversation I had with [redacted] last week before she left for vacation. Valerie Caproni has asked NSLB to determine how many times FISA Roving authority has been granted since the change in the law. [redacted] told me that you were compiling that information and other, similar, statistics. When you get the number, could please send it to us? b6 b7C

Thanks for your help.

~~SECRET~~

Best,
[redacted]

==========

[redacted]
Assistant General Counsel
National Security Law Branch
FBIHQ Room 7975
Direct Line: [redacted]
Unclassified Fax: [redacted]
Secure Fax: [redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted](OGC) (FBI) b6
Sent: Wednesday, March 16, 2005 2:15 PM b7C
To: [redacted]OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted](OGC) (FBI) [redacted] (OGC) (FBI)
Subject: RE: 215, NSL etc

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Which question(s) do you want me to answer? #!1? #4?

[redacted] b5

[redacted] b5

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Wednesday, March 16, 2005 2:06 PM
To: [redacted](OGC) (FBI) [redacted](OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted](OGC) (FBI) b6
Subject: FW: 215, NSL etc b7C

UNCLASSIFIED
NON-RECORD

[redacted]

I really need you to put this together.
Let me know if you can meet this deadline.

b6

[redacted] b7C

Could you assist [redacted]

[redacted]

b6

[redacted] b7C

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Thursday, March 17, 2005 5:30 PM
To: Caproni, Valerie E. (OGC) (FBI)
Subject: RE: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

yes.

-----Original Message-----
From: Caproni, Valerie E. (OGC) (FBI)
Sent: Thursday, March 17, 2005 1:43 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

Can you have the list of 215 orders ready by 3/25?
-----Original Message-----
From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website [redacted] under the "Legislation of Interest" link. b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and

examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, March 16, 2005 11:35 AM
To: [redacted](OCA) (FBI)
Cc: [redacted](OGC) (FBI)
Subject: RE: DOJ Final Draft Report re Patriot Act Sunset Provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

b6 , b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Thanks [redacted] when do you need our comments, if any. Julie

-----Original Message-----
From: [redacted](OCA) (FBI)
Sent: Tuesday, March 15, 2005 6:51 PM
To: THOMAS, JULIE F. (OGC) (FBI); [redacted](OGC) (FBI)
Subject: DOJ Final Draft Report re Patriot Act Sunset Provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

b6
b7C

Julie and [redacted] - attached is DOJ's final draft report to Senate Judiciary re the Patriot Act provisions scheduled to sunset. It's being circulated for final comments this week, with an anticipated dissemination date of 3/30/05. In the last go-around, NSLB didn't have any comments - but I wanted to give you an opportunity for a final look. If you could pay particular attention to the discussion of the FISA provisions, I would really appreciate it. Call if you have questions, Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, February 21, 2005 2:51 PM
To: [redacted](OGC) (FBI)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

Did I already forward this to you? Haven't we already commented on this once? Julie
-----Original Message-----
From: [redacted](OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To: [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted](OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

b6
b7C

[redacted] and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcmte on Terrorism and is meant to:
1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments to [redacted] ext. [redacted] by **9:00 am, Tuesday, 2/22/05**.

b2
b6
b7C

Thanks for your assistance.

-[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, February 22, 2005 8:26 AM
To: [redacted](OCA) (FBI)
Cc: [redacted](OGC) (FBI); BEERS, ELIZABETH RAE (OCA) (FBI)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

I reviewed the attached legislation on behalf of NSLB and have no comments.

Julie Thomas

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

-----Original Message-----
From: [redacted](OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To: [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted]OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

b6
b7C

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcmte on Terrorism and is meant to:
1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments to [redacted]ext.[redacted]by **9:00 am, Tuesday, 2/22/05**.

b2
b6
b7C

Thanks for your assistance.

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Friday, February 11, 2005 5:47 PM
To: [redacted] (OCA) (FBI)
Subject: RE: NSLB Review of DOJ Draft Legislation

b6
b7C

UNCLASSIFIED
NON-RECORD

It will be me. Thanks, Julie

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

-----Original Message-----
From: [redacted] OCA) (FBI)
Sent: Friday, February 11, 2005 5:46 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: NSLB Review of DOJ Draft Legislation

b6
b7C

UNCLASSIFIED
NON-RECORD

Julie - reference our conversation yesterday concerning the need to identify an NSLB attorney to assist with review of DOJ material in connection with efforts relating to the USA Patriot Act reauthorization. I have copies of 4 drafts circulated by DOJ for component comment. I need NSLB's comments by noon on 2/18/2005 to meet DOJ's deadline. As I mentioned on the phone, DOJ considers this material extremely sensitive and has instructed us to limit dissemination. Please identify an NSLB point of contact and I will deliver the material. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, January 19, 2005 1:49 PM
To: [redacted] (OGC) (OGA) b6
Cc: [redacted] (OCA) (FBI) b7C
Subject: RE: sunset

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Great. [redacted], let me know if you need anything else from us. Julie b6 b7C

-----Original Message-----
From: [redacted] (OGC) (OGA)
Sent: Wednesday, January 19, 2005 1:46 PM
To: THOMAS, JULIE F. (OGC) (FBI) b6
Cc: [redacted] (OCA) (FBI) b7C
Subject: sunset

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie:

[redacted] and I just spoke and agreed that we would take out the sublist of USA Patriot Act provisions that will sunset and just refer to them generally. [redacted] will send DOJ our comments concerning the significant purpose standard in FISA. b6 b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, December 15, 2004 3:13 PM
To: [redacted](OGC) (FBI)
Cc: [redacted](OGC) (FBI); [redacted]OGC) (FBI); [redacted](OGC) (FBI); [redacted]OGC)(FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

So, [redacted] will you put together a sample letter with an EC to the field regarding its use for our approval and dissemination? Thanks, Julie

b6
b7C

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Tuesday, December 14, 2004 11:16 AM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](ITD) (FBI); THOMAS, JULIE F. (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

b5

[redacted]

b5

[redacted]

b5

[redacted]

b5

[redacted] b5

[redacted] b5

[redacted] b5

[redacted] I think it is a good idea for OGC to review these requests before they go out to ensure compliance with 2702, since the facts will change in each case. Thanks. Dan b5

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, December 10, 2004 9:45 AM
To: [redacted](OGC) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

FYI
-----Original Message-----
From: [redacted](ITD) (FBI)
Sent: Monday, November 15, 2004 8:05 PM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Cc: [redacted](ITD) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

Unless I hear back otherwise, given everyone's comments, I will reply back to the USAO that FBI OGC is reviewing the matter and that they should inform the local FBI agents that they should not send out the letter without first conferring with FBI OGC NSLB.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel.
Fax [redacted]

b2
b6
b7C

-----Original Message-----

b6
b7C

From: (OGC) (FBI)
Sent: Monday, November 15, 2004 11:43 AM
To: OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI);
(ITD) (FBI)
Subject: RE: 207208 letter

UNCLASSIFIED
NON-RECORD

b6
b7C

Since the pony sent refers to ITOS II, let me see what I can find out from my end.

-----Original Message-----
From: OGC) (FBI)
Sent: Monday, November 15, 2004 10:46 AM
To: THOMAS, JULIE F. (OGC) (FBI); (OGC) (FBI);
(ITD) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

comments.
-----Original Message-----
From: (OGC) (FBI)
Sent: Monday, November 15, 2004 10:35 AM
To: (OGC) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

b5
b6
b7C

I have never seen this. I agree with

-----Original Message-----
From: (OGC) (FBI)
Sent: Monday, November 15, 2004 9:10 AM
To: OGC) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

What do you think?
-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 15, 2004 8:36 AM
To: OGC) (FBI); OGC) (FBI)
Subject: FW: 207208 letter

UNCLASSIFIED

b6
b7C

NON-RECORD

Dear [redacted] and [redacted] b6 b7C

Please note the attachments from [redacted] Is this letter one we have approved ? Please advise,

Julie

-----Original Message----- b6
From: [redacted] (ITD) (FBI) b7C
Sent: Friday, November 12, 2004 4:01 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted] (ITD) (FBI); [redacted] Steven (OGC) (FBI)
Subject: FW: 207208 letter

UNCLASSIFIED
NON-RECORD

Attached is a copy of a form letter sent to me via one of the U.S. Attorney's Offices [redacted] b5

Is this an OGC/NSLB approved letter?

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Science & Technology Law Unit b2
Engineering Research Facility b6
Bldg 27958A, Room A-207 b7C
Quantico, VA 22135
Tel
Fax [redacted]

-----Original Message-----
From: [redacted] (ITOD)(CON)
Sent: Friday, November 12, 2004 8:59 AM b6
To: [redacted] (ITD) (FBI) b7C

Subject: 207208 letter

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, November 16, 2004 12:35 PM
To: [redacted](ITD) (FBI) b6 b7C
Subject: RE: 207208 letter

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Sounds good. Julie

-----Original Message-----
From: [redacted](ITD) (FBI) b6
Sent: Monday, November 15, 2004 8:05 PM b7C
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted](OGC) (FBI)
Cc: [redacted](ITD) (FBI)
Subject: RE: 207208 letter

UNCLASSIFIED
NON-RECORD

Unless I hear back otherwise, given everyone's comments, I will reply back to the USAO that FBI OGC is reviewing the matter and that they should inform the local FBI agents that they should not send out the letter without first conferring with FBI OGC NSLB.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Science & Technology Law Unit b2
Engineering Research Facility b6
Bldg 27958A, Room A-207
Quantico, VA 22135 b7C
Tel.[redacted]
Fax.[redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, November 15, 2004 11:43 AM
To: [redacted](OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted](ITD) (FBI)
Subject: RE: 207208 letter b6 b7C

UNCLASSIFIED
NON-RECORD

Since the pony [redacted] sent refers to ITOS II, let me see what I can find out from my end. b6 b7C

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Monday, November 15, 2004 10:46 AM
To: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (ITD) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] comments.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 10:35 AM
To: [redacted] OGC) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

I have never seen this. I agree with [redacted]

b5
b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 9:10 AM
To: [redacted] (OGC) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

What do you think?

-----Original Message-----
From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 15, 2004 8:36 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

Dear [redacted] and [redacted]

Please note the attachments from [redacted] Is this letter one we have approved and if so, are [redacted] concerns valid? Please advise,

b6
b7C

Julie

-----Original Message-----

b6
b7C

From: [redacted] (ITD) (FBI)
Sent: Friday, November 12, 2004 4:01 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted] (ITD) (FBI); [redacted] (OGC) (FBI)
Subject: FW: 207208 letter

UNCLASSIFIED
NON-RECORD

Attached is a copy of a form letter sent to me via one of the U.S. Attorney's Offices.

[redacted]

b5

Is this an OGC/NSLB approved letter?

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]

b2
b6
b7C

Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel.
Fax [redacted]

-----Original Message-----
From: [redacted] (ITOD)(CON)
Sent: Friday, November 12, 2004 8:59 AM
To: [redacted] (ITD) (FBI)
Subject: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

b6 b7C

From: [redacted]
b6 **To:**
b7C **Date:** Thu, Jun 13, 2002 5:38 PM
Subject: Re: Issues for the Director's upcoming testimony

[redacted] **per your request**

[redacted] b5

[redacted] b5

[redacted] b5

4) The Patriot Act Section 207, (after the initial 120 day order), allows search warrants against 'agents of a foreign power" to remain valid for one year. [redacted]

[redacted] **b5**

Had I had more time, I would have provided additional comments but I hope my theme is fairly clear.

SSA [redacted] b6 b7C

>>> [redacted] 06/12 9:27 AM >>>
Good morning everyone. [redacted] was kind enough to allow me to use her computer to reach out to all of you. My name is [redacted] I work at the Office of Public and Congressional Affairs (OPCA). Part of my duties is to gather information for the Director, so that he may be prepared when he testifies at Capitol Hill. The Director is going to the Hill on Tuesday (6/18/02). b6 b7C

[redacted] b2 b7E

b6
b7C

From: [redacted]
To:
Date: 8/16/02 10:15AM
Subject: Re: Request for Assistance from the CDCs

Albany Division:

[redacted] (S) b1 b2 b7E

No other provisions have been used. Thanks. [redacted]

b6
b7C

>>> [redacted] 08/15 12:02 PM >>>

Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted]

[redacted] 8/22/02

b6
b7C

FYI - responses re: Patriot Act from the CDCs. [redacted]
will send you an e-mail.

[redacted]

~~SECRET~~

b6 b2
b7C b7E

From:
To:
Date: 8/15/02 4:56PM
Subject: Re: Request for Assistance from the CDCs

I was on vacation and out of office. Received this on Tuesday.

(S)

(S)

(S)

b1
b2
b7E
b5
b6
b7C

Hope this helps. Any questions beep me Friday will be doing legal instruction for several squads in b2

b2 b7E

>>> 08/15 12:02 PM >>>
Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

b6
b7C

Please respond to this request by COB tomorrow. Thank you.

~~SECRET~~

[redacted] Re: Request for Assistance from the CDCs Page 1

b6 From: [redacted] [redacted] b2 b7E
b7C To:
Date: 8/16/02 5:03PM
Subject: Re: Request for Assistance from the CDCs

b1 [redacted] (S)
b2 in this e-mail. thanks.
b7E

>>> [redacted] 08/15 11:02 AM >>>
Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

b6
b7C

Please respond to this request by COB tomorrow. Thank you. [redacted]

DATE: 12-19-2005
CLASSIFIED BY 65179DMH/LPCWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

~~SECRET~~

b6
b7C

[redacted] b2 b7E

b1
b2
b7E
b6
b7C

From: [redacted] b6
To: b7C
Date: 8/15/02 5:29PM
Subject: Re: Request for Assistance from the CDCs

[redacted] (S)

>>> [redacted] 08/15/02 12:02PM >>>
Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

b6
b7C

Please respond to this request by COB tomorrow. Thank you. [redacted]

b6
b7C

CC: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6 b2 [redacted]
b7C b7E
From: [redacted]
To:
Date: 8/15/02 3:36PM
Subject: Re: Request for Assistance from the CDCs

Hi [redacted] b6 b7C

b1 [redacted] (S)
b5

I am currently TDY in the National Press Office this week and at least next as well. I will stop to say hello - so be prepared to hide! Thanks [redacted] b6 b7C

>>> [redacted] 08/15 12:02 PM >>>
Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this. b6 b7C

Please respond to this request by COB tomorrow. Thank you. [redacted] b6 b7C

CC: [redacted]

DATE: 12-19-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

b6 [redacted] b2
b7C b7E

From: [redacted]
To:
Date: 8/19/02 11:27AM
Subject: Re: Request for Assistance from the CDCs

b1 b2 b7E [redacted] (S)

b6 b7C >>> [redacted] 8/15 12:02 PM >>>

Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted] b6 b7C

b6 b2
From: b7C [redacted] b7E [redacted]
To:
Date: 8/16/02 4:04PM
Subject: Request for CDC Assistance re: Patriot Act statistics

Dear [redacted]

Per your request [redacted] canvassed its Counterterrorism Squads to provide information regarding the following two questions: b2 b7E

1) How many times have the squads used the tools provided by the Patriot Act

2) Do the Patriot Act tools need refinement/tweaking

The response regarding Question #1:

-Squads made extensive use of the expanded ability to share criminal investigative information under Section 203(d) to enhance liason with local, state, and other federal agencies. The willingness of agencies to participate in Joint Terrorism Task Forces was greatly aided by the ability to share information.

-Squads used Section 214 with the changed standard of "relevance to an ongoing investigation" to obtain pen register and trap and trace orders more readily.

The response regarding Question #2:

-The squads do not have any input to add at this time..

CC: [redacted] b6 b7C

b6 b7C b2 b7E b1 b2 b6 b7C b7E

From: [redacted]
To:
Date: 8/15/02 12:33PM
Subject: Re: Request for Assistance from the CDCs

[redacted] I sent [redacted] response to [redacted] I think [redacted] (S)

b6 b7C

>> [redacted] 08/15 12:02 PM >>>

Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted]

b6 b7C

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

From: [redacted]
To:
Date: 8/12/02 3:39PM
Subject: Re: Message to all CDCs/ADCs

b1
b2
b7E

[redacted] (S)

b6
b7C
b2
b7E

>>> [redacted] 08/01 9:06 AM >>>
Please forward the attached to all CDCs/ADCs. Thanks. [redacted]

b6
b7C

DATE: 12-19-2005
CLASSIFIED BY 65179DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

~~SECRET~~

b6
b7C
From: [redacted]
To: [redacted]
Date: 8/16/02 5:18PM
Subject: Re: Request for Assistance from the CDCs

b2
b7E

[redacted]

b2
b7E
b6

Sorry for the delay in responding, I don't recall receiving the August 1 e-mail. I've queried the [redacted] Supervisors and all have responded negatively. That is, the [redacted] has not taken advantage of the provisions of the Patriot Act yet. All Supervisors recognize the importance of these provisions and will not hesitate to take advantage when the need arises. [redacted]

b6
b7C

>> [redacted] 08/15/02 12:02PM >>>
Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted]

b6
b7C

b6
b7C
From. [redacted]
To: [redacted] b2 b7E
Date: 8/15/02 4:48PM
Subject: Re: Message to all CDCs/ADCs

b1
b2
b6
b7C
b7E

Hi [redacted]

[redacted] (S)

Thanks,

[redacted]

>>> [redacted] 8/01 8:06 AM >>>
[redacted] Please forward the attached to all CDCs/ADCs. Thanks. [redacted] b6 b7C

b6
b7C

From: [redacted]
To: [redacted]
Date: 8/19/02 10:06AM
Subject: Re: Request for Assistance from the CDCs

[redacted]

Sorry for the delayed repsonse. We were having trouble getting a response from the squads that make use of these provisions of the Patriot Act, but for what it is worth, here is what we finally got.

The most helpful provisions of the Act and the ones used most regularly are the nationwide execution of search warrants and the ability to use the same 2703(d) order for multiple companies. The squad could not provide an exact number but said the ability to serve the same court order on multiple companies is used almost every time they serve an order because it is normal to find the first company served is not in fact the ultimate service provider.

Both CT squads were of the opinion the most useful addition would be administrative subpoena authority in both computer crime cases and for phone records in terrorism cases at a minimum.

[redacted]

b2
b6
b7C
b7E

b2
b7E

DATE: 12-19-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]

From b6 [redacted]
To: b7C
Date: 8/13/02 4:29PM b2
Subject: Re: Fwd: Message to all CDCs/ADCs b7E

[redacted] I hope the following information is helpful regarding the "tools" the [redacted] has used post Patriot Act:

[redacted] (S)

b1
b2
b7E

I hope this is what your looking for! Let me know if you need additional information. Thanks!!! [redacted]

b6 >>> [redacted] 08/13 3:26 PM >>>
b7C

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-19-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

7/29/2002

To: SAC [redacted] b6 b7C

From: CDC [redacted]

Subject: SAC's Conference

As we discussed, I'm providing you this information for the upcoming SAC's conference. [redacted] b5

[redacted] b5

[redacted] b5

[redacted] b5

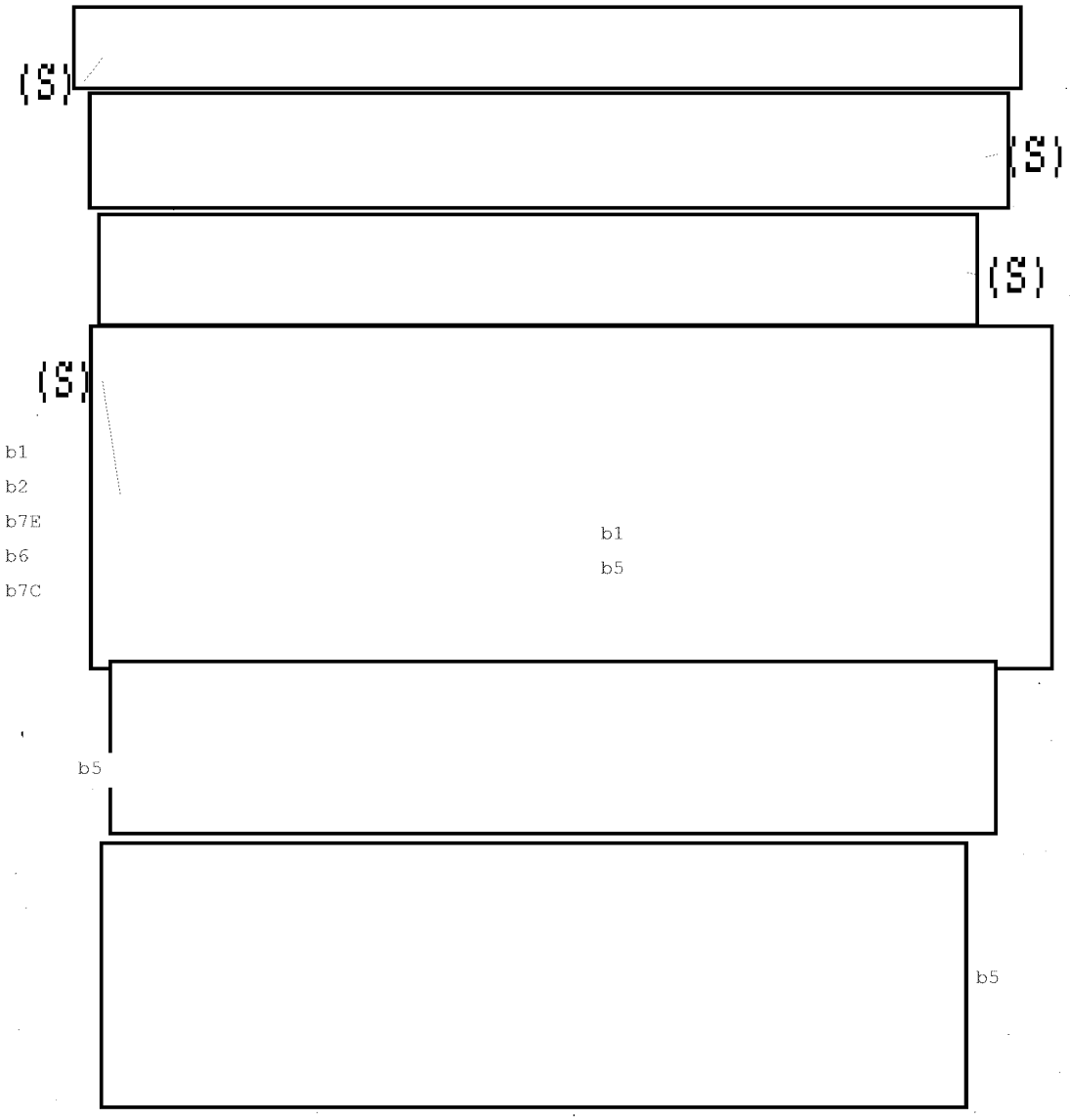
Enclosed are the following which provide examples to help you make your case:

Enclosure 1: My memo to OPCA, dated 6/14/2002. The memo sets out **ten changes that would greatly improve matters.**

~~SECRET~~

[redacted] (S)

b1
b5
b6
b7C
b2
b7E


(S)
(S)
(S)
(S)
b1
b2
b7E
b6
b7C
b1
b5
b5
b5

Enclosure 1

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-19-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

6/14/2002

b6 To: SSA [redacted]

b7C From: CDC [redacted]

b2

b7E Subject: Issues for the Director's Upcoming Testimony

[redacted]

b1
b2
b7E
b5

(S)

[redacted]

~~SECRET~~

b5

Enclosure 1

b5

b5

b5

A few years ago I personally made some of these legislative recommendations to Director Freeh when he visited

b5
b2
b7E

Enclosure 2

DATE: 12-14-2005
CLASSIFIED BY 65179 /DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-14-2030

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

7/29/2002

b2
b7E
b6
b7C

To: CDC

From: SA

Subject:

(S)

(S)

b1
b5

(S)

b1
b2
b6
b7C
b7E

05-CV-0845

(S)

Enclosure 2

~~SECRET~~

Enclosure 3

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-14-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C 05-CV-0845)
DECLASSIFY ON: 12-14-2030

07/29/2002

b6 To: CDC
b7C From: SA
Subject:

(S)

(S)

b1
b2
b6
b7C
b7E

(S)

(S)

(S)

(S)

(S)

(S)

(S)

* Attached Documents

Enclosure 3

b6
b7C

DATE: 12-14-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C 05-CV-0845)
DECLASSIFY ON: 12-14-2030

From: [redacted]
To:
Date: 8/1/02 10:46AM
Subject: Briefing on the Patriot Act

b2
b7E [redacted]

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

[redacted]

In my ever vigilant attempt to be responsive to inquiries on the Patriot Act, I have been tracking its usage and asking questions as best I can. The following is a summary of how we have used the Act and where tweaking is needed.

b1
b2
b6
b7C
b7E

Usage -

[redacted] (S)

(S) [redacted] (S)

[redacted] (S)

Tweaking -

b5 [redacted]

Hope this helps.

[redacted]
b6
b7C

SECRET

[redacted]

From: [redacted]
To:
Date: 8/16/02 12:01PM
Subject: Re: Request for CDC assistance

Sorry for deleting [redacted] email !!! Here's the relevant information. I did not see from your email in what format you wanted this but here it is in a nut shell (I can reformat it and provide greater detail if you need it):

b1
b2
b6
b7C
b7E

[redacted] (S)

>>> [redacted] 08/14 5:07 PM >>>
[redacted] As discussed, see attached. Thanks [redacted]

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2 [redacted]
b7E

~~SECRET~~

b6 From:
b7C To: [redacted]
Date: 8/15/02 2:03PM
Subject: Re: Request for Assistance from the CDCs

DATE: 12-14-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C 05-CV-0845)
DECLASSIFY ON: 12-14-2030

b1 [redacted] (S)
b2
b7E The overall perception about the changes in the Patriot Act:

[redacted] b5

[redacted] b5

[redacted] b5

>>> [redacted] 08/15/02 09:02AM >>> b2 b7E
Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted] b6 b7C

~~SECRET~~ [redacted] b2 b7E

b6
b7C

05-CV-0845

From: [redacted]
To:
Date: 8/15/02 5:17PM
Subject: Patriot Act response

1) NSD-2 is using the increased NSL authority to obtain and identify subscribers of phone numbers in touch with our FFI subjects this is a great enhancement of our FCI cases; we have not had occasion to use 202, 203 206, 207, 209, 210, 211, 212, 213, 214, 217, 218, 219, 220. For 216 we have trap/trace authority now on our FISAs, but I thought that happened before Patriot Act, most of the problem with this is that we can only [redacted]

b2 [redacted] For 215 we have not yet come across a need for it, although one of our current cases may
b7E be our first attempt to use it (separately I sent you a question which will impact our decision to use it, so it may be an issue for others---i.e. the security of using it.)

2) It seems that basic investigation such as obtaining business records, which can be done with admin subpoenas in criminal cases, is made unnecessarily cumbersome when requiring a probable cause FISA standard for CI/CT basic investigation. Not only that, but making the request something other than an administrative subpoena, only heightens its profile to the receiving company, who then knows that it is not a routine criminal investigation.

b6 PS [redacted] is your first name misspelled in e-mail address [redacted] or in LA directory [redacted]?
b7C

[redacted]

[redacted]

b6
b7C

Fr... [redacted]
To:
Date: 8/15/02 6:20PM
Subject: Fwd: Re: PATRIOT ACT FEEDBACK

1) How are we using the tools provided by the Patriot Act?

b5 [redacted]

2) Do these tools require further refinement/tweaking and how?

b5 [redacted]

[redacted]
Office
Pager
Nextel [redacted]

b2
b6
b7C

b6 **From:** [redacted]
b7C **To:**
Date: 8/15/02 7:39PM
Subject: Patriot Act Feedback

[redacted]

b2 [redacted]
b7E

b5 We have not have used any of the other provisions of the Act.

If you need more, or clarification...let me know [redacted] b6
b7C

b6
b7C

From: [redacted]
To:
Date: 8/15/02 8:51PM
Subject: Patriot Act Response

Section 210 updated section 2703(c) and expanded the narrow list of records that we could obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. This capability has greatly increase our ability to rapidly identify computer criminals and trace their Internet connections.

The section also clarifies the we can use a subpoena to obtain the "means and source of payment" that a customer uses to pay for his or her account with a communications provider, "including any credit card or bank account number." This had been a problem in the past and is particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information.

b5 [redacted]

Thanks,

[redacted]
(voice)
(fax)
(mobile)
(pager)

b2
b6
b7C

b6 SECRET
b7C

From: [redacted]
To:
Date: 8/15/02 7:44PM
Subject: patriot act feedback

[redacted]

b1 [redacted] I sent the info to [redacted]
b6 We did not use any of the provisions in Counterintelligence cases. I'd like more info regarding the Title 50 changes or enhancements for future reference. Couldn't find any documentation here. (S)
b7C Please call if you need more information or clarification.

[redacted]

SECRET

DATE: 12-19-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C 05-CV-0845)
DECLASSIFY ON: 12-19-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

To: ADC [redacted]

Fm: SSA [redacted] b6 b7C

Re: Routing Slip and attachment dated 8/13/03

b1
b7E
b2

[redacted] (S)

[redacted] (S)

[redacted] (S)

DATE: 12-19-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

From:
To:
Date: Thu, Aug 15, 2002 7:03 PM
Subject: Patriot Act

b1
b6
b7C
b2
b7E

[redacted] (S)

Thanks [redacted]

~~SECRET~~

[redacted] b2 b7E

Investigative tools under Title 2 of the Patriot Act:

2) Enhanced Surveillance Procedures, Section 203(d), Authority to share criminal investigative information (50 U.S.C. §401a)

b1 b2 b7E [redacted] (S)

This is the first time the Patriot Act has been used in an investigation or [redacted] and time will be needed to evaluate the results of the Act.

b2 b7E

b2 b2E [redacted] Responses to Patriot Act Questionnaire

(S)

b1
b2
b7E

[redacted]

SECRET

[redacted] b2 b7E

b6 From: [redacted]
b7C To:
Date: 8/15/02 12:15PM
Subject: Re: Request for Assistance from the CDCs

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]
b1
b2
b7E

(S)

DATE: 12-19-2005
CLASSIFIED BY 65179DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

b6
b7C

>> [redacted] 08/15 11:02 AM >>>

Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted]

CC: [redacted] b6 b7C

SECRET

b6
b7C

[redacted] b2 b7E

From: [redacted]
To:
Date: 8/1/02 10:59AM
Subject: Re Patriot Act tools

Regarding #11 on your list canvassing on use of the Patriot Act tools, which allows us to get a court order for certain business records for foreign intelligence purposes, I had tried to check a couple weeks ago if NSLU or OGC had produced a sample court order (kind of like they did with the NSL letters), but couldn't find one. It looks like the new provision allows us to go to certain Magistrate judges to obtain this order, but I'm not sure if authority has been delegated to SACs- I guess if SACs don't have the authority to seek this kind of court order, than the field doesn't need a sample. This is just a question and doesn't involve any tweaking of the provision. Thanks!

b6
b7C

From: [redacted]
To: [redacted]
Date: 8/14/02 7:00PM
Subject: Re: Message to all CDCs/ADCs

b2
b7E

[redacted]

b2
b7E
b6

[redacted] survey produced negative results.

Thanks

[redacted]

b6
b7C

>>> [redacted] 08/01 8:06 AM >>>
[redacted] - Please forward the attached to all CDCs/ADCs. Thanks. [redacted]

b6
b7C

[redacted] b2 b7E

From: [redacted]
To: b6
Date: 8/16/02 5:48PM
Subject: b7C Re: Request for Assistance from the CDCs

b2 [redacted]
b7E [redacted] CDC [redacted] asked me to reply to your email today. After speaking with supervisors
b6 and agents assigned to our three terrorism squads in Newark, it seems that the PATRIOT Act has had only a light impact on terrorism investigations here.

b7C Agents have found the following to be beneficial:

b5 [redacted]

[redacted]

Other than these benefits, agents have not experienced any difference in the way they are conducting investigations. [redacted]

b5 [redacted]

[redacted]

b5 [redacted]

[redacted] b5

If you need any further information, or if I can help in any way, let me know.

b2 Thanks.
b7E ADC [redacted]

b6 >>> [redacted] 08/15 12:02 PM >>>
b7C Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted]

CC: [redacted] b6
b7C

b6
b7C

b2
b7E

From:
To:
Date: 8/15/02 5:46PM
Subject: Re: Request for Assistance from the CDCs

b1
b2
b7E
(S)

b5
b6
b7C
(S)

>>> 08/15 12:02 PM >>> b6 b7C

Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you b6 b7C

DATE: 12-19-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

[redacted] b2
b7E

From:
To: [redacted]
Date: 8/15/02 2:50PM
Subject: Patriot Act

You're right. We are busy. I hope this is what you needed.

[redacted] b6 b7C

Part 2: Enhanced Surveillance Procedures, Section 203(d), Authority to share criminal investigative information (50 U.S.C. Section 401a):

Investigators i[redacted] have benefited from this section during the investigation of a 288B case. Previously, we would not have been permitted to share intelligence information gathered during the course of the 288B investigation. Similary, we would not have received the benefit from Grand Jury information obtained from the criminal side of the house. This prohibition would have severely hampered our ability to investigate both the intelligence and criminal cases on our subject in this very complex case. b2 b7E

We also would have had much more difficulty in obtaining computers from our subject's potential victims because of the prohibition against information sharing. Due to the recent changes, however, we were able to share information with other Federal law enforcement, intelligence, immigration, national defense and national security officials who can help us in accomplishing our goals.

Part 6: Enhanced Surveillance Procedures, Section 210, Scope of Subpoenas for Electronic Evidence (18 U.S.C. 2703(c)(2):

[redacted] (S)
b1
b2
b7E

Part 7: Enhance Surveillance Procdures, Section 211, Clarifying the Scope of the Cable Act (47 U.S. C 551, 18 U.S.C. 2510, 18 U.S.C. 2701, and 18 U.S.C. 3121):

(S) [redacted]
b1
b2
(S) [redacted]

SECRET (S) [redacted]

b1
b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-19-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

Part 11: Enhanced Surveillance Procedures, Section 215, Access to Records and other items under the FISA (50 U.S.C. 1861):

[redacted] (S)

b1
b7E
b2

b6 b7C b2 b7E [redacted]

From: [redacted]
To:
Date: 8/19/02 2:53PM
Subject: CDC Request re Patriot Act Enhancements

DATE: 12-19-2005
CLASSIFIED BY 65179/DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

[redacted]

I returned today after a prolonged absence. Here is a brief narrative response as to what provisions have been used in some manner since the passage of the Act. If not listed, the provision has not been employed yet, to my knowledge. This is less than precise, but it's something.

Section 203(d) [sharing of info]: We have an active JTTF, which includes representatives of INS and Customs, and this provision has facilitated the approriate sharing of info.

Section 210 [scope of subpoenas for electronic evidence]: Our GJ subpoenas commonly incorporate the new language, and it is of course especially relevant when they are directed to ISPs.

Section 213 [delayed notice of execution of SW] [redacted] (S)

b1 b2 b7E b5

Section 214 [redacted] (S) b1 b2 b7E

Section 216 [title 18 pens]: We have drafted many of the pens, including pens directed to ISPs, and have incorporated the revisions. Helpful.

As some of our international and domestic case develop, I fully expect [redacted] will make use of the other provisions. b2 b7E

[redacted] b6 b7C

SECRET

b6
b7C
b2
b7E

DATE: 12-19-2005
CLASSIFIED BY 65179 DMH /LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

From:
To:
Date: 8/19/02 11:08AM
Subject: Patriot Act

Sorry for the late response (everyone seems to be on vacation, including me). Anyway, nothing of note here regarding investigative tools under the Patriot Act.

1. We are now seeking a FISA using the extended duration from Section 207. The agents feel the new time limits are a big help.

b1
b2
b7E
b5

(S)
(S)
(S)
(S)
(S)
(S)

Hope this helps.

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-19-2005
CLASSIFIED BY 65179DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

SECRET

b6
b7C

From: [redacted]
To:
Date: 8/15/02 3:04PM
Subject: Patriot Act

b2
b7E [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2 b7E The following is [redacted] response to the questions posed in your August 1, 2002 request for information:

1) How are we using the tools provided by the Patriot Act?

b1
b2
b7E [redacted] (S)

2) Do these tools require further refinement/tweaking and how?

[redacted] does not have any suggestions on refinement or tweaking of the Patriot Act.

b2
b7E

[redacted]

CC: b6 b7C [redacted]
b2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SECRET

DATE: 12-19-2005
CLASSIFIED BY 65178DMH /LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

05-CV-0845 b6 b7C

b2 b7E

From:
To:
Date: 8/15/02 12:26PM
Subject: Re: Request for Assistance from the CDCs

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

b1 b2 b6 b7C b7E

(S)

(S)

b6 b7C >>> 08/15 9:02 AM >>>

Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. b6 b7C

b6
b7C

[redacted]
b2
b7E

From: [redacted]
To:
Date: 8/9/02 9:20AM
Subject: Re: Fwd: Message to all CDCs/ADCs

After querying all agents, I have (incredibly) no use to report.

[redacted]

b6
b7C

>>> [redacted]8/01 9:10 AM >>>
Please see attached message from UC [redacted] Please respond directly to [redacted]

Thank you.

b6
b7C

From: [redacted]
To:
Date: 8/9/02 1:23PM
Subject: Patriot Act use ...

I originally reported that [redacted] had no input. Well, that changed. Here it is:

b2 (S)
b7E

Section 207 [redacted]

Section 214 [redacted]

b1
b2 [redacted] (S)
b7E

Section 215 [redacted]

b1 (S)
b2 [redacted]
b6
b7E
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-19-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C 05--CV-0845)
DECLASSIFY ON: 12-19-2030

b6
b7C

From: [redacted]
To:
Date: 8/19/02 11:14AM
Subject: Patriot Act Provisions

[redacted]

A quick canvass of our squad shows that we have used or considered use of the following Sections of the Patriot Act as listed in your recent query.

#	Section
2)	203(d)
6)	210
7)	211
13)	217
16)	220

b5 [redacted]

I left a message with AUSA [redacted] and will update this response if new information is obtained.

b6
b7C

CC: [redacted]

DATE: 12-19-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

b6
b7C

b2
b7E

From:
To:
Date: 8/16/02 4:31PM
Subject: USA Patriot Act

(S)

b1
b2
b6
b7C
b7E

CC:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

b2
b7E

From:
To:
Date: 8/12/02 6:38PM
Subject: Investigative tools under the Patriot Act

The roving FISA authority (Section 206)

b1
b2
b7E

(S)

Section 218

b1
b2
b7E

(S)

DATE: 12-19-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C [redacted] b2 b7E

From:
To: [redacted]
Date: 8/16/02 12:35PM
Subject: Re: Request for Assistance from the CDCs

[redacted]

b6 My apologies for not responding sooner, but I have been out of town and this week we've had some
b7C Congressional staffers here (including former [redacted]). But to answer your questions on the Patriot Act, there are areas that we have used extensively in San Diego and have had a positive impact on our ability to work CT cases.

Section 203(d) allows for information sharing in counter terrorism cases. We have a Joint Terrorism Task Force and other close direct contacts with various intelligence agencies and state law enforcement organizations that could not operate without close coordination between the officers and agents of these various groups.

Section 207 has been helpful in extending the time to conduct FISA surveillance.

Section 505 provided for the delegation of National Security Letters authorization to the SAC level. This has been used extensively in San Diego.

[redacted] b5 b2 b6 b7C

>> [redacted] 08/15/02 09:02AM >>>

b6 Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your
b7C assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you [redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C
b2
b7E [redacted]

From: [redacted]
To:
Date: 8/16/02 2:32PM
Subject: Patriot Act

DATE: 12-19-2005
CLASSIFIED BY 65179 DNH LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

[redacted] I am apologize, this response is late. I did not get much in the way of a response from the request I sent out to my supervisors.

b1
b2
b7E

[redacted] (S)

I am sorry I don't think this was particularly helpful.

[redacted]
b6
b7C

[redacted] b2 b7E

From: [redacted]
To:
Date: 8/16/02 3:23PM
Subject: Re: Request for Assistance from the CDCs

b1 (S) [redacted] b2 b7E

>> [redacted] 08/15 1:02 PM >>>

Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you. [redacted]

b6 b7C

~~SECRET~~

[redacted] - Re: Request for Assistance from the CDCs Page 1

[redacted] b2 b7E

b6 b7C **From:** [redacted]
To:
Date: 8/19/02 8:40PM
Subject: Re: Request for Assistance from the CDCs

Ok, although I'd like to have gotten you something a little more polished, in the interest of giving you something here goes:

b1 b2 b7E [redacted] (S)

b1 b2 b7E (S) [redacted]

b5 [redacted]

Sorry for not getting this to you sooner.

I still want to touch base re my upcoming meeting with the [redacted] I'll try you later (fair warning). b6 b7C

Thanks, G

>>> [redacted] 08/15 9:02 AM >>>

b6 b7C Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

Please respond to this request by COB tomorrow. Thank you [redacted]

~~SECRET~~

b6
b7C

[redacted]

b2
b7E

From.. [redacted]
To:
Date: 8/19/02 9:15AM
Subject: Re: Request for Assistance from the CDCs

[redacted]

b6
b7C

I was out of the division last week. Recently retired [redacted] previously sent out this request to applicable supervisors, but I did not receive any responses before I left. I have resubmitted it and will send you any positive information I receive. Thanks.

[redacted]

>> [redacted] 08/15 12:02 PM >>>
Good morning: Attached is a communication that was sent to you on August 1, 2002, requesting your assistance in obtaining information regarding the Patriot Act in response to a request from Senators Feinstein, Leahy and Kyl for a briefing of their staffers. In particular, the questions posed are how many times have we have used the tools provided by the Patriot Act and if the tools need refinement/tweaking. (the tools are listed in the attachment). The briefing is scheduled for August 20. We requested responses by August 14, 2002, so as to give us adequate time to prepare. As of today we have not received responses from you. I know you are extremely busy but it is imperative that we obtain information to respond to the 2 questions posed by the Senators. Congress has specifically requested this information and it is important that we be as comprehensive and accurate as possible in our response. Plus, this is an opportunity to attempt to obtain revisions, if necessary, to better the tools. We need to provide them with statistics and examples to accomplish this.

b6
b7C

Please respond to this request by COB tomorrow. Thank you. [redacted]

b6
b7C

b2
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-19-2005
CLASSIFIED BY 65179 DMH/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-19-2030

From:
To:
Date: 8/15/02 12:29PM
Subject: Use of Patriot Act

SECRET

b6
b7C

Here's what I have come up with. There's probably more, but these are the responses received.

(S)

b1
b2
b7E

This is all I have for now.

b6
b7C

SECRET

From: [redacted] b6 b7C
To:
Date: 8/1/02 5:28PM
Subject: Fwd: Re: Issues for the Director's upcoming testimony

[redacted]

These were my comments in June and little has changed.

---

b6 SSA [redacted]
b7C [redacted]
b2
b7E Privileged and Confidential

CC: [redacted]

b6
b7C

I know you have busy schedules. I apologize for such short notice. I have a few questions that I would like to put to you. Perhaps, you can answer them. Please send your replies to me, so that I do not burden [redacted] any further. We have to prepare the briefing book for the Director before week's end.

#1. Are you aware of any terrorist events that the FBI has thwarted? Please provide examples.

b6
b7C
b2

#2. Are you aware of any terrorist investigations that were hampered by the old Attorney General Guidelines (i.e., not being able to enter places of worship; or, political impediments). Please provide examples.

I appreciate any help you may provide. Thank you. [redacted]

If you can answer the following questions, please reply to [redacted] at OPCA.

#1. Which aspects of the Patriot Act need tweaking?

#2. Provide specific detail and statistics as to how the Patriot Act has been used (e.g., number of wiretaps, searches, etc.).

Thank you.

b2
b6
b7C

[redacted]

CC: [redacted]

b6
b7C

From: [redacted]
To:
Date: 8/19/02 12:42PM
Subject: Fwd: Re: PATRIOT ACT FEEDBACK

[redacted]

We have provided training on the Patriot Act to Supervisors and Agents. As you know, there are some Agents who when given the opportunity will always complaint about something. We also have additional training coming up on aspects of the Patriot Act but we are still waiting on the final version of the of policy that is undergoing review by NSLU and OIPR. (Sharing of FISA and Grand Jury information).

b2 [redacted]
b7E

>>> [redacted] 08/19/02 05:31AM >>>

b6 [redacted] Thanks for all the extra input you were able to obtain. It is extremely helpful.
b7C

Just a note - I am a little concerned that there may be agents in LA that believe the Patriot Act has not yet been implemented (see forwarded e-mail). Both ILU and NSLU sent out ECs providing guidance on the Patriot Act (see attached) and I know the CDCs have been using the materials OGC provided you at the CDC Conference in January for guidance and training. Please feel free to re-circulate the attached ECs if you think it may be beneficial. Thanks again for all your help. [redacted]

b6 >>> [redacted] 08/16/02 09:36PM >>>
b7C FYI

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-19-2005
CLASSIFIED BY 65179DMH/LP/CWC
REASON: 1.4 (C 05-CV-0845)
DECLASSIFY ON: 12-19-2030

b6
b7C

From: [redacted]
To:
Date: 8/8/02 2:23PM
Subject: Staff Brief re: Patriot Act

Thanks for the information.

Also --- this may be obvious, but: please note specifically in your e-mail that this is an important matter, that Congress has specifically requested this information, & that it's important that we be as comprehensive & as accurate as possible in our response.

Thanks.

>> [redacted] 08/08/02 02:11PM >>>

[redacted] (S)

b1
b2
b6
b7C
b7E

[redacted] (S)

[redacted] (S)

All the other responses have addressed tweaking the act. I will send a reminder e-mail out tomorrow.

b6
b7C

[redacted]

SECRET

b6
b7C

DATE: 12-08-2005
CLASSIFIED BY 65179DMH/LP/cpb
REASON: 1.4 (c)
DECLASSIFY ON: 12-08-2030

CA# 05-CV-0845

[redacted] (OGC) (FBI)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-06-2005 BY 65179 DMH/CLS

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:03 PM
To: [redacted] (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] I. (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

UNCLASSIFIED
NON-RECORD

b6
[redacted] I can provide you the results from the field survey that OGC conducted, however, I can also guarantee that b7C
these are not entirely accurate numbers. The field survey was voluntary, and the level of detail provided varied between the field offices. Furthermore, since then I have been advised that some HQ divisions have been utilizing various Patriot Act tools, and I did not receive any contributions from any HQ division on this survey, so their use is not included in any numbers that I have.

The field offices reported the following: (S) (S) (S) b1
Section 206 - Roving FISA orders [redacted] times b2
Section 215 - Used [redacted] times, [redacted] additional orders currently in approval process b7E

Section 213 - Delayed Notice for Search Warrants - This is not a sunset provision, so we did not seek field input on this specific provision at this time.

Also - as you are aware, field offices collect statistics on their accomplishments (i.e. search warrants executed). I believe that Finance Division maintains, compiles, and reports these statistics. They may have more accurate field wide numbers.

I hope this is helpful.

[redacted] b2
Assistant General Counsel b6
Investigative Law Unit
Office of the General Counsel b7C
[redacted]

-----Original Message-----
From: [redacted] (Div00) (FBI)
Sent: Tuesday, May 18, 2004 1:41 PM
To: BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] Div09) (FBI); [redacted] Div09) (FBI)
Cc: [redacted] (Div00) (FBI) b6
Subject: Statistics re USA PATRIOT Act provisions b7C
Importance: High

UNCLASSIFIED
NON-RECORD

In anticipation of the Director's scheduled appearance before the Senate Judiciary Committee this Thursday, May 20th, we are trying to confirm the number of times we have used Delayed Notice (so-called "Sneak and Peek") Warrants, FISA Roving Wiretaps, and FISA Orders for Tangible Things (i.e., so-called

Section 215 Orders), since passage of the USA PATRIOT Act.

I realize there are several potential complications with compiling such numbers (e.g., Delayed Notice Warrants used in traditional criminal cases, classification issues re 215 Orders, etc.). Nevertheless, if any of you could provide some input on this, it would be very helpful. We can almost guarantee the Director will be asked about the numbers when he testifies.

Is DOJ compiling numbers? Is there anyone at OLP or OIPR who may know?

Thanks,

[redacted]
Office of Congressional Affairs
ext. [redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

b6
b7C

[redacted](OGC) (FBI)

From: [redacted](OGC) (FBI)
Sent: Friday, July 16, 2004 2:26 PM
To: KELLEY, PATRICK W. (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)
Cc: Caproni, Valerie E. (OGC) (FBI); [redacted](OGC) (FBI)
Subject: FW: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

Pat: This is the final compilation of OGC-gathered examples and comments on the provisions of the Patriot Act that will sunset in Dec 2005 unless they are made permanent. This was collected for a variety of reasons--mainly for DOJ/OLP and it contributed to the report DOJ issued the other day. Now, OCA needs it and [redacted] needs it [redacted] is the point person on that) to respond to Sen Feinstein's inquiries. I need to send it to [redacted] in OCA and who will put it into the format they want. Before I do I am sending it to you for official blessing with a copy to Spike who said he would look to see if [redacted] rewrite (she took out names, places, etc from the case summaries she recieved) would allow us to declassify it.

b2
b6
b7C

[redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, July 16, 2004 1:41 PM
To: [redacted](OGC) (FBI)
Subject: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] - Attached is the final version. If you have any questions, please feel free to contact me.

[redacted]

b6
b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
DECLASSIFICATION EXEMPTION 1
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
DECLASSIFICATION EXEMPTION 1
~~SECRET//ORCON,NOFORN~~

b6
b7C

[redacted] (OGC) (FBI)

From: KELLEY, PATRICK W. (OGC) (FBI)
Sent: Tuesday, July 20, 2004 11:22 AM
To: [redacted] (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)
Cc: Caproni, Valerie E. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] I assume you've coordinated the intercept issues with TLU. Two comments: The first paragraph at the top of p. 8 seems to be missing something; there's not even a period. Also, in the 2nd paragraph on p. 8, and on p. 10, we mention delays attributable to OIPR. While true enough, it would probably be more prudent to delete the references to OIPR and just leave it as "processing delays." Otherwise, it's good to go by me.

b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, July 16, 2004 2:26 PM
To: KELLEY, PATRICK W. (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)
Cc: Caproni, Valerie E. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

b2
b6
b7C

Pat: This is the final compilation of OGC-gathered examples and comments on the provisions of the Patriot Act that will sunset in Dec 2005 unless they are made permanent. This was collected for a variety of reasons--mainly for DOJ/OLP and it contributed to the report DOJ issued the other day. Now, OCA needs it and [redacted] needs it ([redacted] is the point person on that) to respond to Sen Feinstein's inquiries. I need to send it to [redacted] in OCA and who will put it into the format they want. Before I do I am sending it to you for official blessing with a copy to Spike who said he would look to see if [redacted] rewrite (she took out names, places, etc from the case summaries she recieved) would allow us to declassify it.

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, July 16, 2004 1:41 PM
To: [redacted] (OGC) (FBI)
Subject: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] Attached is the final version. If you have any questions, please feel free to contact me.

b6
b7C

[redacted]

~~**DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations**~~
~~**DECLASSIFICATION EXEMPTION 1**~~

~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET//ORCON,NOFORN~~

b6
b7C

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Tuesday, July 20, 2004 11:30 AM
To: [redacted] (OGC) (FBI)
Subject: FW: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] I made the corrections as per Pat's e-mail, and it is attached. I'm not sure what "intercept issues" he is referring to that involve TLU.

b5
b6
b7C

[redacted]
-----Original Message-----
From: KELLEY, PATRICK W. (OGC) (FBI)
Sent: Tuesday, July 20, 2004 11:22 AM
To: [redacted] (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)
Cc: Caproni, Valerie E. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

b6
b7C

[redacted] I assume you've coordinated the intercept issues with TLU. Two comments: The first paragraph at the top of p. 8 seems to be missing something; there's not even a period. Also, in the 2nd paragraph on p. 8, and on p. 10, we mention delays attributable to OIPR. While true enough, it would probably be more prudent to delete the references to OIPR and just leave it as "processing delays." Otherwise, it's good to go by me.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, July 16, 2004 2:26 PM
To: KELLEY, PATRICK W. (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)
Cc: Caproni, Valerie E. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

Pat: This is the final compilation of OGC-gathered examples and comments on the provisions of the Patriot Act that will sunset in Dec 2005 unless they are made permanent. This was collected for a variety of reasons--mainly for DOJ/OLP and it contributed to the report DOJ issued the other day. Now, OCA needs it and [redacted] needs it [redacted] is the point person on that) to respond to Sen Feinstein's inquiries. I need to send it to [redacted] in OCA and who will put it into the format they want. Before I do I am sending it to you for official blessing with a copy to Spike who said he would look to see if [redacted] rewrite (she took out names, places, etc from the case summaries she recieved) would allow us to declassify it.

b2
b6
b7C

[redacted]
-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, July 16, 2004 1:41 PM
To: [redacted] (OGC) (FBI)
Subject: Sunset provisions - Examples

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] - Attached is the final version. If you have any questions, please feel free to contact me. b6

[redacted] b7C

DERIVED ~~FROM: G-3~~ FBI Classification Guide G-3, dated 1/97, ~~Foreign Counter~~Intelligence Investigations
DECLASSIFICATION EXEMP~~TION 1~~
SEC~~RET//ORCON~~,NOFORN

DERIVED ~~FROM: G-3~~ FBI Classification Guide G-3, dated 1/97, ~~Foreign Counter~~Intelligence Investigations
DECLASSIFICATION ~~EXEMP~~TION 1
SECRET//ORCON,NOFORN

~~DERIVED~~ FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence ~~Investigations~~
DECLASSIFICATION EXEMPTION ~~1~~
~~SECRET//ORCON,NOFORN~~

~~DERIVED FROM~~: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence ~~Investigations~~
DECLASSIFICATION EXEMPTION 1
~~SECRET//ORCON~~,NOFORN

b6
b7C

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Tuesday, July 20, 2004 12:20 PM
To: [redacted] (OCA) (FBI)
Cc: BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); Curran, John F. (OGC) (OGA); [redacted] (OCA) (FBI)
Subject: Sunset provisions

b6
b7C

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] attached are our comments and the results of our field and HQ survey on the Patriot Act sunset provisions. We folded in the examples provided by NSLB so it is one complete OGC package. [redacted] kept the classification she received for the examples but she deleted most of the references to subject's names, locations,etc--so I am sure that much what is labled SECRET can be declassified--but I can't do that, which is why I copied Spike.

b6
b7C

Not knowing what format you wanted, I just sent it as is. DGC Pat Kelley has approved it as well.

[redacted]
Office of the General Counsel
[redacted]

b2
b6
b7C

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFY ON: 20140720~~
~~SECRET//ORCON,NOFORN~~

Use of the USA PATRIOT Act
Classified Appendix

Section 212 - Emergency Disclosure of Electronic Communications to Protect Life and Limb

- [redacted] (S)

~~SECRET~~

CA# 05-CV-0845

Examples of Patriot Act Use
Requiring Additional Facts

Section 201 - Expanded predicate offenses for T-3

[redacted]- FO initiated [redacted] T-3 in a 315 case where terrorism identified as a predicate offense. Was this the only predicate offense? Would we have been able to get the T-3 without the Patriot Act change?

[redacted]- improved ability of info sharing with state/locals/ and other federal agencies in order to respond rapidly to threat and make an action plan.

[redacted]-

[redacted] info sharing with others critical

[redacted] info sharing with others critical

b2
b7A
b7E

Section 203 - Information Sharing (from criminal to the intell side)

[redacted]- 315Q-[redacted]-56983

[redacted]

[redacted] - 315N-[redacted]-33992

[redacted]

315O-[redacted]-215590

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 01-03-2006
CLASSIFIED BY 65179 dmh/baw 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 01-03-2031

[redacted]- This provision used most notably in the following cases:

[redacted]

[redacted]- 315B-[redacted]-52073

[redacted]

[redacted]-[redacted]

315Q-[redacted]-57173 -

b2
b6
b7A
b7C
b7E

Section 206 - Roving FISAs

[redacted]- I received the following from the CDC on the case recently released to the press regarding the plot to blow up a shopping mall. [redacted]

"I believe we used the roving FISA on [redacted] not [redacted] These are related cases, but two seperate cases, file numbers and FISA requests. I believe the roving part [redacted] As far as [redacted] [redacted] so you can use as much of the press release information as you would like."

b2
b7A
b7E

b2
b6
b7A
b7C
b7E

~~SECRET~~

Any clarification on this case would be helpful.

Section 212 - Emergency Disclosures by ISPs
[redacted]- 315S-[redacted]-224164
also used in a case regarding a "threat to a high ranking foreign official"

Section 214 - new standard for FISA pen/trap (S)
[redacted]- used [redacted] different 315 cases; ASAC notes that this was "extremely helpful" and could not have been obtained without the new pen/trap standard.

[redacted]- A pen/trap order was obtained [redacted] Any updates to this case?

[redacted] - 65A-[redacted]-220066

[redacted] - 315N-[redacted]-68267 - pen on [redacted]
65M-[redacted]-66909 - pen not possible under old standard [redacted]
[redacted] via the pen
[redacted] pen obtained on subject [redacted]

[redacted] - 315N-[redacted]-57048 - likely not to obtain pen/trap under old standard

Section 218 - Change in the Primary Purpose Standard for FISA
[redacted]- AUSAs have worked closely to identify criminal charges against the subject [redacted]

[redacted]- the [redacted] and [redacted] Investigation - FO states that even though information had been passed over "the wall" prior to the wall coming down and an indictment was being prepared, when the "wall" came down, significantly more information was passed to the criminal investigators and prosecutors giving them a clearer understanding of the case.

[redacted]- There are [redacted] other 315 cases where information sharing has been critical to the success of the investigations.

[redacted] - 315N-[redacted]-56807 (S)

[redacted] - 315Q-[redacted]-36062

b2
b7E

[redacted] - 315M-[redacted]-45821

[redacted]

281F-[redacted]-66686 - having criminal side fully apprized of all of the intelligence assisted in the coordination [redacted] b2 b7A b7E

[redacted] - direct result of info sharing, subject was arrested without incident

315N-[redacted]-67573

[redacted]-[redacted] criminal activity determined and cases opened b2 b7A b7E

Section 220 - Nationwide search warrants for e-mail

[redacted]-[redacted] b2 , b7A, b7E

[redacted] - used in the [redacted] investigation b2 , b6, b7C, b7E

[redacted]-[redacted]- Significant part of [redacted] This expedited the receipt of critical information. b2 b7A b7E

~~SECRET~~

DATE: 12-06-2005
CLASSIFIED BY 65179/DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 09-08-2005

(OGC) (FBI)

From: (Div09) (FBI) b6
Sent: Friday, March 12, 2004 2:42 PM b7C
To: (Div09) (FBI) CA# 05-CV-0845
Subject: RE: 2702(b)(7) Emergency Request *Secret* For Director's information.

UNCLASSIFIED
NON-RECORD

DATE: 12-06-2005
CLASSIFIED BY 65179/DMH/ LP/ CWC
REASON: 1.4 (c)
DECLASSIFY ON: 12-06-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Yes it's classified. Since being Trilogized, we're still trying to figure out how to send emails. I sent it unclassified, non-record so that I could send it out, but I marked Secret in the Subject line. There you go - clear as mud.

b2
b6
b7C

Assistant General Counsel
National Security Law Branch
Counterterrorism Law Unit 1

-----Original Message-----
From: Div09) (FBI) b6
Sent: Friday, March 12, 2004 1:50 PM b7C
To: (Div09) (FBI)
Subject: RE: 2702(b)(7) Emergency Request *Secret* For Director's information.

UNCLASSIFIED
NON-RECORD

Thanks!! I'm a little confused. I assume this is classified info. Am I correct? I plan to mark it at the secret level and submit it with the remainder of examples. It will go through the front office of OGC and then over to DOJ Office of Legislative Affairs. Is this OK?

b6 b1
-----Original Message----- b7C b2
From: (Div09) (FBI) b7E
Sent: Friday, March 12, 2004 12:34 PM b6
To: Div09) (FBI) b7C
Cc: Div09) (FBI)
Subject: 2702(b)(7) Emergency Request *Secret* For Director's information.

UNCLASSIFIED
NON-RECORD

(S)

Assistant General Counsel
National Security Law Branch
Counterterrorism Law Unit 1

~~SECRET~~

b6
b7C

(OGC) (FBI)

From:
Sent: Monday, March 08, 2004 1:16 PM
To: Div09) (FBI)
Cc: (Div09) (FBI); (Div09) (FBI); (FBI); Div09) (FBI);
Subject: Re: PATRICT ACT SUNSET PROVISIONS

Sensitivity: Private

CA# 05-CV-0845

1) FISA Business records - The FBI and DOJ should hang their heads in shame that this potentially useful authority has NEVER been used (at least it should be easy for HQ to count). The Patriot Act passed in 10/2001 and almost 3 YEARS later OGC and OIPR can't decide what pleadings to file. Meanwhile the militant librarian lobby keeps kicking us around because they "think" we use this authority. Given the apparent "shock and awe" effect of angry librarians on FBIHQ - WFO reccmmends that this useless authority IMMEDIATELY sunset - it would be less frustrating for the SAs and the librarians will stop picking on HQ.

2) FISA Roving authority - This authority is also a complete waste. Damm shame - it was intended to be a robust tool similar to the criminal T-III roving (read Sen Leahy's 2001 summary) but it NEVER roves. What we have is non-roving roving authority. stopped asking for it - a waste of effort. Its simply pathetic that OIPR turned this potentially useful tool into a cartoon of what it should have been. As explained by Mike Woods after his brefing on the Hill - roving authority would attach to the Target and when the target picked up a phone we were aurhtorized to intercept. yeah right - OIPR turned it into "Motionless Authority"

b2
b7E

3) FISA Pen Register - the OIPR approval delays have rendered this tool almost useless. Its OIPR's last priority and the SAs no longer bother to use it. We will do without or find a way to use the criminal authority

b2
b7E

SSA
WFO Office of Division Counsel x

Privileged and Confidential

b2
b6
b7C

>>> (Div09) (FBI) 03/04 3:17 PM >>>
UNCLASSIFIED
NON-RECORD

See the attached EC that was uploaded today. See 66F-HQ-1364260-5.

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Friday, March 12, 2004 6:45 PM
To: [redacted] (Div09) (FBI)
Subject: RE: Patriot Act

b6
b7C

CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
RECORD 66F-HQ-C1364260

[redacted] - Attached are the two documents. One is classified, the other contains LE Sensitive material because it discusses ongoing cases. I've marked the paragraphs, but I'm not sure I used the proper techniques. I assume there is someone that can do that for us on Monday.

b6
b7A
b7C

Also - I was advised that they used the emergency disclosure provision on the [redacted] So I did not include it in my list.

Finally - I also attached a copy of a document that [redacted] forwarded to me previously on sneek-n-peek cases that DOJ put together. I include a copy, in the event that the POC in OLP is not aware of this document. I also put a paper copy of the [redacted] press release in your in box. I reference this in the document.

If you have any questions, feel free to call me at home. I should be home in the morning until 11 and then again after 1pm.

Thanks.

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Thursday, March 11, 2004 11:06 AM
To [redacted] (Div09) (FBI)
Subject: Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] when you get in tomorrow, I need you to collect all that you can of examples, stats, etc on all the Patriot Act provisions--not just the sunset ones. We need to get it to DOJ (OLP) by Monday. Thought we had more time which is why I set the 3/19 deadline for the sunset EC--but we don't so we'll do what we can. We'll just have to follow up later with the responses to the EC. Let's talk first thing and discuss how to do this.

b6
b7C

[redacted]

[redacted]
Office of the General Counsel
[redacted]

b2
b6
b7C

UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

Use of the USA PATRIOT Act

Section 210 - Scope of Subpoena

- This provision expanded the type of information that can be obtained from an Internet service provider (or other types of service providers) with a subpoena. This expansion allows agents working computer intrusion cases to immediately identify if a computer used by a hacker is a victim computer where the hacker is 'hoping through' the computer, or is the computer hacker's own computer. This significantly expedites computer intrusion investigations. Referral/Direct

- [redacted]

Section 212 - Emergency Disclosure of Electronic Communications to Protect Life and Limb

[redacted] b1 b2 b7E (S)

- [redacted] b2 b7A b7E

- **Recent Kidnaping Case** - Recently, a 14 year old girl was abducted. Her laptop was also missing. The case agents suspected that the nefarious character she had met in an Internet chat room was the perpetrator. [redacted] e-mail. As a result, the suspect was quickly identified and interviewed. He admitted to picking up the girl and took agents to the truck stop where he had left her. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours. This is but one example of how essential this provision is for child abduction b7A

~~SECRET~~

cases.

Section 216 - Nationwide Effect of Pen/Trap Orders

- **(LE SENSITIVE)** **Hacker** - are becoming more widespread throughout both corporate and private systems. This computer hacker

b2
b7A
b7E

(LE SENSITIVE) In this case it was difficult to identify the hacker because he each time he entered the corporate victim's computer because he was each time. Due to the changes in Section 216 of the USA PATRIOT Act, the FBI was able to obtain for this hacker and then present it to This enabled the agents to identify the hacker. He was recently arrested and is awaiting trial. (LE SENSITIVE)

b7A

Section 217 - Interception of Computer Trespasser Communications

-

b2
b7A
b7E

- **(LE SENSITIVE) U.S. Government System Hacked** - Recently a U.S. Government computer system was identified as the victim of a computer hacker. The hacker was utilizing the government computer to The

b2
b7A
b7E

investigation is ongoing to identify the suspect and any additional victims. (LE SENSITIVE)

Section 814 - Deterrence and Prevention of CyberTerrorism

- [redacted]

b2
b7E

[redacted] (OGC) (FBI)

From: [redacted]
Sent: Friday, March 19, 2004 3:04 PM
To: [redacted](Div09) (FBI)
Subject: [redacted] PATRIOT Act Use Report

b2
b6
b7C
b7E

CA# 05-CV-0845

patriotact-use-ilu.w
pd (15 KB)...

[redacted] Attached is an electronic copy of [redacted] PATRIOT Act Use Report. A hardcopy will follow in the Bureau mail.

[redacted]

b2
b6
b7C
b7E

[redacted] OGC) (FBI)

From: [redacted] b2
Sent: Friday, March 19, 2004 3:29 PM b6
To: [redacted] Div09) (FBI)
Cc: [redacted] b7C
Subject: Patriot Act sunset provisions ... b7E
Importance: High

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-21-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

patriot act sunset provisions ... [redacted]

b6
b7C

The deadline for submission of our response is today. To assure timely receipt, the [redacted] Division response is attached. ACS and paper copies will follow. b2 b7E

Please note that the EC is classified "SECRET."

[redacted]

b6
b7C

b6 , b7C

[redacted] (OGC) (FBI)

From: [redacted]
Sent: Friday, March 26, 2004 11:42 AM
To: [redacted]
Cc: [redacted]
C. (Div09) (FBI)
Subject: Another tasking

[redacted] b2 b6 b7C b7E

FBIHQ requests a brief write-up of significant cases aided by the Patriot Act. Some of it is sun setting. Please provide me with a brief write-up of the big [redacted] Case and [redacted] in [redacted] Please list file numbers. The document to FBIHQ will be classified if need be (probably).

Please list all sophisticated techniques used. I know FISAs (electronic and physical), T-IIIs (new predicates/information sharing), e-mail SWs(now nationwide allowed), NSLs(SAC authority), GJ subpoenas (information sharing), SWs(nationwide for terrorism; delayed notification), etc were used in these cases. Please list some significant accomplishments in these cases. Also, obviously, information sharing has aided in coordinating the criminal side and FCI side of the cases.

I know [redacted] case effort has resulted in an entire network being identified and cases being initiated nationally and overseas. Also, we've probably issued hundreds of NSLs for the [redacted] case. Please give me rounded number of NSLs if it is available. b2 b7E

For the [redacted] case, it will be mentioned that the overseas seizing power and subpoena power was contemplated, although not in the end used (I don't think). b7A

We don't think we are using the PATRIOT Act , but since it altered the statutory authority of every one of our investigative techniques, we use it everyday. FBIHQ wants specifics on big cases to report back to the security committees on how these new tools are being used. Please help. Lee.

Anyway, I don't want to add to your already big loads, but if you have a write-up handy with some statistics on number of techniques, and other accomplishments, I can add the rest. I'll forward the final copy.

[redacted]

CC: [redacted] OGC
b6
b7C

SECRET/ORCON/NOFORN

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 04/26/2004

To: General Counsel **Attn:** Investigative Law Unit
Room 7326

From: [redacted]
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

b2
b6
b7C
b7E

Case ID #: (U) 66F-HQ-C1364260
(U) 66F-HQ-C1384970
(U) AL 66F-A3035

Title: (U) USA PATRIOT ACT
SUNSET PROVISIONS

Synopsis: (U) Case narratives provided as requested.

~~(S)~~ (U) ~~Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) 66F-HQ-C1364260 Serial 5

b2
b7E

Details: ~~(S)~~ (U) As requested in referenced EC, [redacted] is providing the following case narratives which describe investigations aided by provisions of the USA Patriot Act.

[redacted]

(S)

b1
b2
b7A
b7E

SECRET/ORCON/NOFORN

b2
b7E

To: General Counsel From:
Re: (U) 66F-HQ-C1364260, 04/26/2004

b1
b2
b6
b7A
b7C
b7E

PATRIOT ACT PROVISIONS USED:

*Section 201 and 202 - Title III Predicates - no new predicates used in case but Title IIIs extensively used.
*Section 203 Information Sharing.
*Section 209 regarding voice mail.
*Section 220 regarding nationwide Search Warrants for E-Mail.

(S)

(S)

To: General Counsel From:
Re: (U) 66F-HQ-C1364260, 04/26/2004

b1
b7A

(S)

PATRIOT ACT PROVISIONS USED:

*Section 203, Information Sharing
*Section 214, New Standard for FISA Pen/Trap
*Section 218 & 504, Changes to "Primary Purpose" Standard for FISA

~~(S)~~ (S)
~~(S)~~ (S)

b1
b2
b7A
b7E

(U) In October 2001, JTTF initiated investigation into Investigation was predicated on Source information which was corroborated by information provided by CAU, FBIHQ.

b2
b7A
b7E

(S) ~~(U)~~ subjects have been convicted on heroin related and fraudulent document charges including two State Department of Motor Vehicles employees. Numerous investigative techniques were utilized which included a Title III, 150 consensual recordings, and a

b1
b2
b7E

(U)

b2
b6
b7C
b7E

(U)

b2
b6
b7A
b7C
b7E

 b2

b7E

To: General Counsel From:
Re: (U) 66F-HQ-C1364260, 04/26/2004

(U) b2 b6 b7A b7C b7D b7E

PATRIOT ACT PROVISIONS USED:

*Section 203, Information Sharing
*Sections 201 & 202, Expanded Predicate Offenses for Title III (expanded predicates not used in case, just Title III)

b2 b7A b7E

(U)

(U) b2 b6 b7A b7C b7D b7E

(U)

(S) (S)

b1 b2 b6 b7C b7E

To: General Counsel From:
Re: (U) 66F-HQ-C1364260, 04/26/2004

[redacted] (S)

b1
b2
b6
b7C
b7E

[redacted] (S)

b1
b2
b6
b7C
b7E

PATRIOT ACT PROVISIONS USED:

*Section 203, Information Sharing;
*Section 214, New Standard for FISA Pen/Trap;
*Section 218 & 504, New "Primary Purpose" Standard for FISA

USE OF INFORMATION SHARING AUTHORITY

JOINT TERRORISM TASK FORCE (JTTF)

(U) Original staffing was [redacted] FBI Special Agents (SA's) and [redacted] full-time Task Force Officers (TFO's) of other federal state, and local agencies. Current staffing has grown to [redacted] FBI SA's, sixteen TFO's, and [redacted] Intelligence Analyst [redacted] (IA [redacted] The JTTF currently has full-time representatives from the Department of State (DOS), Internal Revenue Service (IRS), [redacted] Federal Air Marshal [redacted] FAM [redacted] from the Transportation Security Administration (TSA), two SA's from the Immigration & Customs Enforcement (ICE), [redacted] New York State Police (NYSP) Investigators, [redacted] New York State Office of Inspector General Investigator [redacted] and [redacted] Detective [redacted] from

b2
b7E
b7F

[redacted] (OGC) (FBI)

DECLASSIFIED BY 65179 DMH/CLS
ON 09-21-2005

CA# 05-CV-0845

From: [redacted] FBI) b2
Sent: Friday, April 30, 2004 12:56 PM
To: [redacted] (Div09) (FBI) b6
Subject: RE: Patriot Act sunset provisions ... b7C
b7E

~~SECRET~~ (U)
RECORD 66F-HQ-C1364260

[redacted]

I am unfamiliar with the specifics in the case. I sent your e-mail to [redacted] for details.

Please note that we're under an inspection and otherwise extremely busy here! But we'll try to get what you need as scon as we can. b6
b7C

Also, any movement on the emergency pen and trap delegation issue? We recently had another case in which local authority was obtained in a kidnapping case while the FBI pondered using the federal process.

[redacted]

-----Original Message----- b2
From: [redacted] (Div09) (FBI) b6
Sent: Friday, April 30, 2004 12:32 PM
To: [redacted] (FBI) b7C
Subject: FW: Patriot Act sunset provisions ... b7E

~~SECRET~~ (U)
RECORD 66F-HQ-C1364260

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:29 PM b6
To: [redacted]
Subject: RE: Patriot Act sunset provisions ... b7C

~~SECRET~~ (U)
RECORD 66F-HQ-C1364260 b2
b6

[redacted] - Thanks for your submission regarding the sunset provisions. I'm in the process of compiling these for the General Counsel. Do you think you could provide me more details on your Division's use of the Roving FISA surveillance? (see page 2 of your EC). In it you noted that this was used in conjunction with the [redacted] Division to [redacted] I'm wondering what triggered the need for roving surveillance? [redacted] Feel free to label what you want as classified, I'll keep whatever markings you put on it. b7C b7E

Thanks for your help.

[redacted] b6
Assistant General Counsel
Investigative Law Unit b7C
Office of the General Counsel

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, March 19, 2004 3:29 PM
To: [redacted] (Div09) (FBI)
Cc: [redacted]
Subject: Patriot Act sunset provisions ...
Importance: High

b2
b6
b7C
b7E

[redacted]:

The deadline for submission of our response is today. To assure timely receipt, the [redacted] Division response is attached. ACS and paper copies will follow.

Please note that the EC is classified "SECRET."

b2
b6
b7C
b7E

[redacted]

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

SECRET

DATE: 12-07-2005
CLASSIFIED BY 65179 DHM/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-07-2030

[redacted](OGC) (FBI)

From: [redacted](Div09) (FBI)
Sent: Tuesday, May 04, 2004 1:38 PM
To: [redacted](FBI)
Subject: Sunset Provisions

b2
b6
b7C

DATE: 09-21-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 09-21-2030
CA# 05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SECRET//ORCON,NOFORN
RECORD 66F-HQ-C1364260

b6 , b7C

[redacted] I'm still working hard on this. I want to include the following summaries from your EC. I've still classified them as SECRET, but want to ensure that I'm accurately stating the facts. Could you please proof these for me. I included the file number at the end only for your reference. I don't intend to include that with my final version nor that these came from [redacted] (that is for my reference purposes only.)

b2
b7E

Thanks so much for all your help.

b6 , b7C

[redacted]

[redacted] (S)

[redacted] (S)

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET//ORCON,NOFORN

b1
b2
b7A
b7E

SECRET

~~SECRET~~

DATE: 12-07-2005
CLASSIFIED BY 65179 DHM/LP/CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-07-2030

b2
b6
b7C
b7E

[redacted] (OGC) (FBI)

From: [redacted] (FBI)
Sent: Tuesday, May 04, 2004 2:05 PM
To: [redacted] (Div09) (FBI)
Subject: RE: Sunset Provisions

~~DATE: 09-21-2005~~
~~CLASSIFIED BY 65179 DMH/CLS~~
~~REASON: 1.4 (C)~~
~~DECLASSIFY ON: 09-21-2030~~
CA# 05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

I am familiar with this case and information and your written paragraphs accurately state this material. We appreciate your assistance in defending our use of these techniques! [redacted] b6 b7C

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 04, 2004 1:38 PM
To: [redacted] (FBI)
Subject: Sunset Provisions

b2
b6
b7C
b7E

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

[redacted] I'm still working hard on this. I want to include the following summaries from your EC. I've still classified them as ~~SECRET~~, but want to ensure that I'm accurately stating the facts. Could you please proof these for me. I includec the file number at the end only for your reference. I don't intend to include that with my final version nor that these came from [redacted] (that is for my reference purposes only.) b2 b6 b7C

Thanks so much for all your help. b7E

[redacted] b6 , b7C

(S)

(S)

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET//ORCON,NOFORN~~

b1
b2
b7A
b7E

~~SECRET~~

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET//ORCON,NOFORN

[redacted] (OGC) (FBI)

From: [redacted] (FBI) b2
Sent: Thursday, May 06, 2004 12:40 PM b6
To: [redacted] (Div09) (FBI) b7C
Subject: [redacted] example for PATRIOT ACT b7E

~~SECRET~~
RECORD 315N-[redacted]-64028 b2 b7E

[redacted] I hope this meets your needs. Let me know if you need more. Hard copy is in the mail. Thanks [redacted] b6 b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

(Rev. 01-31-2003)

~~SECRET~~ CA# 05-CV-0845

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/30/2004

To: Investigative Law Unit **Attn:** [redacted] b6 b7C

Counterterrorism b2 b7E SSA [redacted]
ITOS I, Conus 4, Tm 16

From: [redacted]
Squad 21
Contact: SSA [redacted]

Approved By: [redacted]

Drafted By: [redacted] aem b2 b6 b7C

Case ID #: (U) 66F-HQ-C1364260 (Pending)

Title: (U) US PATRIOT ACT b2 b7E
SUNSET PROVISIONS

Synopsis: (U) Provide detailed "Tear Line" summary of [redacted] example of the benefits of information sharing, through the PATRIOT ACT, regarding parallel criminal and intelligence cases on one subject.

~~(S) Derived From : G-3~~
~~Declassify On: X1~~

Reference: (U) 66F-HQ-C1364260 Serial 5 b2
(U) 29E-[redacted]-64536 b7E
(U) 315N-[redacted]-64028

Administrative: (U) E-mail from ITOS 1, dated 04/30/04.

Details: (U) Above reference Serial requested offices to provide the Investigative Law Unit (ILU), OGC, with "statistics, good examples or anecdotes... summarizing the benefits the office has received from the (PATRIOT ACT) provisions...." [redacted] complied with this request. [redacted] was recently re-contacted by ILU to provide more details on the example [redacted] provided regarding information sharing. b2 b7E

(U) ~~(S)~~ As requested by ILU, [redacted] is providing ILU with a summary of the parallel criminal and intelligence

~~SECRET~~

investigations regarding subject [redacted] which resulted in the successful prosecution and deportation of the subject.

[redacted] (S)
b1
b2
b7E

(U) Therefore, for the benefit of ILU, [redacted] is providing both a detailed classified summary, followed by a "Tear-Line" summary, approved by [redacted] and ITOS 1, for the use of ILU. b2 b7E

Classified Summary Background: ~~(S)~~

[redacted] (S)
b1
b2
b6
b7A
b7C
b7E

[redacted] (S)

b2

To: ?? From: [redacted] b7E

Re: (U) 66F-HQ-C1364260, 04/30/2004

(S) [redacted]

[redacted] (S)

[redacted] (S)

(U) Outlined below, is an unclassified "Tear Line" summary for the use of ILU.

b1
b2
b6
b7C
b7D
b7E

----------Tear Line----------

Unclassified

Summary Background: In the aftermath of the September 11th terrorist attacks, a subject, [redacted]

To: ?? From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 04/30/2004 b7E

[redacted] was identified by a reliable asset as [redacted] among a group of Islamic extremists residing in the US. The Subject was an outspoken supporter of Osama Bin Laden and a self-proclaimed admirer of the September 11th terrorists. Early inquiries into the Subject's background disclosed the fact that [redacted] b2 b6 b7C b7E

Due to Subject's extremist views, affiliations with other terrorism subjects, [redacted] Therefore, cited criminal case was opened. Early investigations confirmed that [redacted] b2 b7E

As noted above, the subject was initially identified as a terrorist subject through asset reporting. Upon receipt of this asset information regarding his financial activities, a separate criminal investigation was opened. During the criminal investigation, asset reporting was continually passed to the criminal investigators to provide investigative lead information and important background and behavioral assessment information. Additionally, timely asset information also assisted in the successful planning and execution of Subject's arrest, after it

was determined that Subject was planning on leaving the country on short notice.

----------Tear Line----------

Set Lead 1: (Info)

COUNTERTERRORISM

AT WASHINGTON, D.C.

To: ?? From: [redacted] b2
Re: (U) 66F-HQ-C1364260, 04/30/2004 b7E

(U) For information.

Set Lead 2: (Info)

GENERAL COUNSEL

AT WASHINGTON, DC

(U) For information.

[redacted](OGC) (FBI)

From: [redacted](Div09) (FBI) b6

Sent: Tuesday, May 11, 2004 5:23 PM b7C

To: [redacted](Div09) (FBI)

Subject: Sunset Provisions

~~SECRET~~
RECORD 66F-HQ-C1364260

b6
b7C

[redacted]- Attached are the two documents I provided to OPA [redacted] The 1st document is the summary of the field survey that I'm currently putting together. I did leave in the classified portions for you. The 2nd document was a brief summary we provided to DOJ in March.

The consistent comment from the field was that the information sharing provisions (203 and 218) were the most important provisions in the Patriot Act. As you know, they have significantly altered the way we conduct business on a daily basis. This was a consistent point made in the field responses. They pointed to the joint task forces, better communications with other agencies, better working relationships across the board because they are no longer stifled by fear that they may inadvertantly share information incorrectly, better use of resources, etc.

While we know that 218 opened the door for more communications from the intell to the criminal side, does NSLB have any opinion on what effect the expiration of 218 would have on the FISC court opinion? Would this essentially then rebuild the wall?

If I can help, please feel free to contact me.

[redacted]
x[redacted]

b2
b6
b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
DECLASSIFICATION EXEMPTION 1
~~SECRET~~

CA# 05-CV-0845

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 3:08 PM
To: [redacted] (Div00) (FBI)
Cc: [redacted] (Div00) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); BOWMAN, MARION E. (Div09) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE
DATE: 01-03-2006
CLASSIFIED BY 65179 dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 01-03-2031

SECRET

[redacted] please be advised that the use of 215 mentioned below just refers to a field office having submitted requests. As of last week, we still had not received a business record order. There was a possibility that one went through this past Friday to the FISC, and we are still waiting to hear from OIPR as whether this in fact happened. We'll let you know no later than tomorrow what the response is.

b6
b7C

[redacted]

-----Original Message-----
From [redacted] Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:03 PM
To [redacted] (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc [redacted] Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

b6

[redacted] - I can provide you the results from the field survey that OGC conducted, however, I can also guarantee that these are not entirely accurate numbers. The field survey was voluntary, and the level of detail provided varied between the field offices. Furthermore, since then I have been advised that some HQ divisions have been utilizing various Patriot Act tools, and I did not receive any contributions from any HQ division on this survey, so their use is not included in any numbers that I have.

b7C

The field offices reported the following:

b1

Section 206 - Roving FISA orders [redacted] times (S)
(S) Section 215 - Used [redacted] time; [redacted] additional orders currently in approval process (S)

b2
b7E

Section 213 - Delayed Notice for Search Warrants - This is not a sunset provision, so we did not seek field input on this specific provision at this time.

Also - as you are aware, field offices collect statistics on their accomplishments (i.e. search warrants executed). I believe that Finance Division maintains, compiles, and reports these statistics. They may have more accurate field wide numbers.

I hope this is helpful.

[redacted]
Assistant General Counsel

b6
b7C

SECRET

Investigative Law Unit
Office of the General Counsel
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] Div00) (FBI)
Sent: Tuesday, May 18, 2004 1:41 PM
To: BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] Div09) (FBI)
Cc: [redacted] Div00) (FBI)
Subject: Statistics re USA PATRIOT Act provisions
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

In anticipation of the Director's scheduled appearance before the Senate Judiciary Committee this Thursday, May 20th, we are trying to confirm the number of times we have used Delayed Notice (so-called "Sneak and Peek") Warrants, FISA Roving Wiretaps, and FISA Orders for Tangible Things (i.e., so-called Section 215 Orders), since passage of the USA PATRIOT Act.

I realize there are several potential complications with compiling such numbers (e.g., Delayed Notice Warrants used in traditional criminal cases, classification issues re 215 Orders, etc.). Nevertheless, if any of you could provide some input on this, it would be very helpful. We can almost guarantee the Director will be asked about the numbers when he testifies.

Is DOJ compiling numbers? Is there anyone at OLP or OIPR who may know?

Thanks,

[redacted]
Office of Congressional Affairs
ext [redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

SECRET

SENSITIVE BUT UNCLASSIFIED

(OGC) (FBI)

From: (FBI) b2
Sent: Friday, July 02, 2004 1:57 PM b6
To: (OGC) (FBI) b7C
Subject: RE: Sunset Provisions - Roving FISA order b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I believe we used the roving FISA on not These are related cases, but two seperate cases, file numbers and FISA requests. I believe the roving part As far as so you can use as much of the press release information as you would like. b6 b7A b7C

I hope I did not confuse the matter.

b6
b7C

-----Original Message-----
From: (OGC) (FBI) b2
Sent: Tuesday, June 22, 2004 12:01 PM b6
To: (FBI) b7C
Subject: RE: Sunset Provisions - Roving FISA order b7E

b2 b5 b6 b7A b7C b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

- I'm making final revisions to my summary of examples where we used the various Sunset provisions found in the Patriot Act. As you may recall, you had responded that the Now that there has been a public indictment and press release on this case, how would you like me to cover this example? I assume that it is use with the specifics of this case that make it classified. Am I correct?

Thanks for your input. -- (b2 , b6, b7C

-----Original Message-----
From: (FBI) b2
Sent: Monday, May 03, 2004 1:20 PM b6
To: (Div09) (FBI) b7C
Subject: RE: Sunset Provisions - Roving FISA order b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hi the case I was referring to was the case and the spin-off cases against 315N- 71500 and 315N- 71501. The technique used was I believe These cases are still pending and are highly classified due to the FISA and other techniques being used. b2 b6 b7A b7C b7E

b6
b7C

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:07 PM
To: [redacted] (FBI)
Subject: FW: Sunset Provisions - Roving FISA order

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:03 PM
To: [redacted] FBI)
Subject: Sunset Provisions - Roving FISA order

b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] - Thanks for your response to our call to the field for examples using the sunset provisions. I'm compiling the results for the GC. In your EC, you noted that the [redacted] RA JTTF [redacted] Can I get more info on this use? It seems like a good case to include as an example. Also let me know how you want it classified. You noted it was still an ongoing case, so should we classify it? or just label it law enforcement sensitive?

b2
b6
b7A
b7C
b7E

Thanks.

[redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

DATE: 09-26-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 09-26-2030

~~Message~~

~~SECRET~~

CA# 05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Tuesday, July 06, 2004 11:28 AM
To: [redacted] CTD) (FBI) b6 b7C
Subject: Additional case information - Patriot Act Examples

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] b6 b7C b2

In finalizing my summary of Patriot Act examples, I've come across some great cases out of [redacted] however, I need some additional information in order to make the connection to how the Patriot Act provisions were indeed helpful. Is there someone in your office that might be familiar with these cases that I could speak to briefly? b7E

The cases are as follows:

[redacted] (S) b1 b2 b6 b7A b7C b7E

Thank you.

[redacted]
Assistant General Counsel b2
Investigative Law Unit b6
Office of the General Counsel
[redacted] b7C

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
~~SECRET//ORCON~~,NOFORN

~~SECRET~~

[redacted] (OGC) (FBI) CA# 05-CV-0845

From: [redacted] (OGC) (FBI) b6
Sent: Friday, July 02, 2004 3:39 PM b7C
To: [redacted] (CTD) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] OCA) (FBI)
Subject: Case examples for Sunset Provisions of the Patriot Act

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
[redacted] - As per our conversation earlier today, attached please find a WP document which lists many cases b7C
the field offices provided to me as examples of our use of the Patriot Act. I have organized this list based upon the section of the Act that was utilized. For most of these cases, I have very limited information regarding the case, so the case summaries you mentioned would be very helpful. Where I had additional information, I included a brief statement that may assist CTD in determining how the Patriot Act was useful to that case. I hope this is helpful to CTD as they collect examples.

If I can be of further assistance, please feel free to contact me or the National Security Law Branch.

[redacted]
Assistant General Counsel b2
Investigative Law Unit b6
Office of the General Counsel
[redacted] b7C

SENSITIVE BUT UNCLASSIFIED

[redacted](OGC) (FBI)

From: [redacted](OGC) (FBI) b6 b7C

Sent: Tuesday, July 06, 2004 5:49 PM

To: [redacted]OGC) (FBI); [redacted](OGC) (FBI)

Subject: Synopsis of Field Response for use of Patriot Act Sunset Provisions

~~SECRET//ORCON,NOFORN~~
RECORD 66F-HQ-C1364260

[redacted] b6 b7C - Attached is my draft synopsis of the field response to our survey this spring on the use of the sunset provisions to the Patriot Act. As you will see, it includes a brief paragraph describing the provision, general comments from the field anc the number of times the field reported using a provision, along with more specific examples.

I plan to do my final review of this document on Friday morning, however, wanted to provide you an opportunity to review it over the next several days if you desire. I plan to seek OGC approval to release this document to CAO on Friday so that they may respond to the DCI's request for examples.

If you have any questions, I'll be happy to answer them on Friday.

[redacted] b6 b7C

DERIVED FROM: ~~G-3 FBI Classification~~ Guide G-3, dated 1/97, ~~Foreign Counterintelligence~~ Investigations
DECLASSIFICATION EXEMPTION 1
~~SECRET//ORCON,NOFORN~~

[redacted](OGC) (FBI)

From: [redacted](CTD) (FBI)
Sent: Friday, July 09, 2004 1:39 PM
To: [redacted](OCA) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](CD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI); [redacted](OCA) (FBI); [redacted](OCA) (FBI); [redacted](OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted](OCA) (FBI); [redacted](OGC) (FBI)
Subject: RE: Tasking from DCI - Renewed Request for PATRIOT Act Examples

b6
b7C

~~SECRET~~
RECORD 66F-HQ-A1413614-G

b6
b7C

[redacted]

Attached are the case write ups from CTD (ITOS I) that we discussed previously.

[redacted]

b6
b7C

-----Original Message-----
From: [redacted](OCA) (FBI)
Sent: Friday, July 09, 2004 1:04 PM
To: BOWMAN, MARION E. (OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](CTD) (FBI); [redacted](CD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI); [redacted](OCA) (FBI); [redacted](OCA) (FBI); [redacted](OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted](OCA) (FBI); [redacted](OGC) (FBI)
Subject: RE: Tasking from DCI - Renewed Request for PATRIOT Act Examples

b6
b7C

UNCLASSIFIED
NON-RECORD

I agree that we should not try to meet during Director Tenet's visit. Will 11:00 work for others? Please let me know via email.

Thanks,

[redacted]

b6
b7C

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Friday, July 09, 2004 11:04 AM
To: [redacted](OCA) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](CTD) (FBI); [redacted](CD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI); [redacted](OCA) (FBI); [redacted](OCA) (FBI); [redacted](OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted](OCA) (FBI); [redacted](OGC) (FBI)
Subject: RE: Tasking from DCI - Renewed Request for PATRIOT Act Examples

b6
b7C

UNCLASSIFIED
NON-RECORD

This turns out to be a bad time as Director Tenet is being presented with an award at that time -- perhaps we could make it 1100?

-----Original Message-----
From: [redacted](OCA) (FBI)
Sent: Thursday, July 08, 2004 3:56 PM
To: [redacted]OGC) (FBI)[redacted]OGC) (FBI); [redacted]OGC) (FBI); [redacted](CTD) (FBI); [redacted](CD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI)[redacted]OCA) (FBI); [redacted]OCA) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted]OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted](OCA) (FBI); [redacted](OGC) (FBI)
Subject: RE: Tasking from DCI - Renewed Request for PATRIOT Act Examples
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

The Community Management staff has inquired about our progress in collecting examples of the FBI's utilizat on of the USA PATRIOT Act provisions that are due to sunset.

I am aware that ILU is preparing a report on the topic that should be largely completed by tomorrow. I am also aware that CTD has solicited some additional examples from field offices, with a deadline of COB tomorrow. I'm unsure whether NSLU has been able to gather any further examples, particularly FISA-related examples. Have the materials I provided from the EOUSA canvass proven helpful in tracking down any related FBI examples?

Please try to collect your best examples for inclusion in the classified report being prepared by the Community Management staff as soon as possible.

Also, please advise whether you would be available to meet with the Community Management reps next Tuesday, July 13 at 10:00 am, to discuss the examples gathered so far, and to agree upon a deadline for the completion of this tasking.

Thank you for your continued assistance on this matter,

[redacted]
OCA
[redacted]

b2
b6
b7C

-----Original Message----
From: [redacted](OCA) (FBI)
Sent: Thursday, July 01, 2004 9:29 AM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted]OGC) (FBI); [redacted](CTD) (FBI); [redacted](CD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI); [redacted](OCA) (FBI); [redacted](OCA) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted](OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted](OCA) (FBI); [redacted](OGC) (FBI)
Subject: RE: Tasking from DCI - Renewed Request for PATRIOT Act Examples
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

Today's meeting has been postponed to allow us more time to firm up the FBI's examples. The meeting will be rescheduled for next week. In the meantime, please continue to review the materials previously provided, and contact the necesary personnel within your respective divisions/units to solicit additional examples of the FBI's utilization of the USA PATRIOT Act.

Thank you,

[redacted] b2
OCA b6
[redacted] b7C

-----Original Message-----
From: [redacted] OCA) (FBI) b6
Sent: Tuesday, June 29, 2004 8:37 AM b7C
To: [redacted] (OGC) (FBI); [redacted] OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (CTD) (FBI); [redacted] (CD) (FBI)
Cc: VAN DUYN, DONALD N. (CTD) (FBI); [redacted] OCA) (FBI); [redacted] (OCA) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted] (OCA) (FBI); KELLEY, PATRICK W. (OGC)(FBI); [redacted] (OCA) (FBI)
Subject: RE: Tasking from DCI - Renewed Request for PATRIOT Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

Due to today's planned evacuation drill, the meeting with [redacted] reps has been postponed until Thursday at 11:00 am. b2

Please advise if you will be able to attend.

Thank you,

[redacted] b2
OCA b6
[redacted] b7C

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Friday, June 25, 2004 11:10 AM
To: [redacted] (CTD) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (CD) (FBI) b6 b7C
Cc: VAN DUYN, DONALD N. (CTD) (FBI); [redacted] OCA) (FBI); [redacted] (OCA) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted] (OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted] (CTD) (FBI); [redacted] (OCA) (FBI)
Subject: Tasking from DCI - Renewed Request for PATRIOT Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

Your assistance is needed on the following tasking:

In letters dated March 23, April 28, and June 14, 2004, Sen. Dianne Feinstein has requested the Attorney General (AG) and the Director of Central Intelligence (DCI) to undertake a comprehensive review of the implementation of the USA PATRIOT Act. Sen. Feinstein's most recent letter, which includes her earlier letters as enclosures, is attached (see email from ExecSec).

Sen. Feinstein's letters coincide with DOJ's own efforts to compile examples of PATRIOT Act successes for congressional testimony, required reports, and related purposes. As most of you know, the FBI has frequently been tasked with collecting such examples.

In an effort to respond to Sen. Feinstein and to create a comprehensive report on the PATRIOT Act that can be used for different purposes, the AG and DCI agreed to the following division of labor: DOJ agreed to prepare a section-by-section legal analysis of the Act and an unclassified report on the Act's implementation. Meanwhile, the DCI (through the Legal Counsel for the Deputy DCI for Community Management) agreed to draft a classified report containing examples of different PATRIOT Act provisions, particularly the sixteen provisions due to expire in 2005.

Drafts of DOJ's section-by-section analysis and the unclassified report are attached. Both of these are in draft form, so they should not be distributed as finished products. Nevertheless, I'm told that both are close to completion.

Earlier this week, the FBI was tasked with providing input for the classified report on the sixteen provisions due to sunset. Specifically, we have been asked to compile ten to fifteen "examples that reflect the FBI's use of these provisions and how they have enhanced the accomplishment of the FBI's mission."

I had hoped that we might already have sufficient examples from prior taskings to satisfy this request, but it appears that we may have purposely avoided compiling classified examples, and many of our unclassified examples have apparently been included in DOJ's draft report. Accordingly, I am seeking your assistance in compiling additional PATRIOT Act examples.

There is some good news here: In the process of preparing the attached unclassified report, DOJ canvassed all of the US Attorneys across the country for examples. While most provided unclassified examples, many also provided classified examples. I met with Matthew Berry in DOJ's Office of Legal Policy and obtained copies of these classified examples. This morning, I will deliver copies of this material, as well as the tasking from the DCI and related materials prepared by the FBI in March, to each of the recipients in the "to" line above.

My preliminary review of the classified materials supplied by US Attorneys suggests we will need to do some follow-up to come up with good examples. Presumably, however, most of the examples are derived from FBI cases, so we should have a good head start.

Ideally, the DCI would like to receive our examples by next Friday, July

2, 2004. [redacted] and FBI Detailee [redacted] are coordinating this effort for the Intelligence Community (IC). They would like to meet with us next Tuesday, June 29, 2004 to talk about the project. I'm hoping that, by Tuesday morning, we can review the materials from DOJ and reexamine any PATRIOT Act examples compiled in response to previous taskings, so they we can provide [redacted] and [redacted] with a realistic estimate of the examples already collected, and the time needed to put them into final form. It is my hope that we may have enough raw material to develop the requested examples, but I will need your input in making this assessment and collecting any additional facts.

b6
b7C

Please respond by email or phone regarding your availability for a meeting on Tuesday morning, June 29, at 10:00 am (here at FBIHQ) to discuss this matter further with our colleagues from the IC. (Those copied on this email are also welcome to attend.)

Thank you very much,

[redacted]
Office of Congressional Affairs
ext. [redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~DERIVED FROM: Multiple Sources~~

~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Friday, July 09, 2004 4:34 PM
To: [redacted] (OGC) (FBI)
Subject: Patriot Act Sunset Provisions: Summary of Field Survey

b6
b7C

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

b6
b7C

[redacted] - Attached is the draft summary of the field survey we conducted seeking input on the sunset provisions. As you are aware, I am continuing to update this with additional examples provided by CTD. However, is OGC sufficiently satisfied with the current version to release this to OCA so that they may develop a response to letters from Senator Feinstein and any other congressional responses as they see fit?

Please feel free to contact me if you have any additional questions.

Thanks --

[redacted]

b2
b6
b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~//ORCON,NOFORN

~~SECRET~~

(OGC) (FBI)

From: (FBI) b2
Sent: Friday, July 09, 2004 5:01 PM b7C
To: (OGC) (FBI) b7E
Subject: FW:
Follow Up Flag: Follow up
Flag Status: Flagged

DATE: 09-26-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 09-26-2030
CA# 05-CV-0845

DATE: 12-07-2005
CLASSIFIED BY 65179 DHM LP CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-07-2030

~~SECRET~~
RECORD b2 , b7A, b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

I heard back from the Case Agent. He's provided the file number of the three cases alluded to in the FISA trap & pen section of 03/19/2004 EC re the use of PATRIOT Act authorities. b2 b6 b7C b7E

b2 , b6, b7C, b7E

-----Original Message-----
From: (FBI) b1
Sent: Friday, July 09, 2004 3:42 PM b2
To: (FBI) b2 , b6, b7C, b7E b7A
Subject: b7E

~~SECRET~~
RECORD b2 , b7A, b7E

(S)

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
~~SECRET~~

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
~~SECRET~~

~~SECRET~~

[redacted] (S)

[redacted] (S)

b1
b2
b7A
b7C
b7E

(U) Background Information:

[redacted] (S)

b1
b2
b6
b7A
b7C
b7E

Section 203 - Information Sharing :

(U) The [redacted] has been utilizing Federal Grand Jury Subpoenas to **obtain financial** records, telephone records, Internet usage and liaison with local law **enforcement** intelligence branches.

b2
b7E

(

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Tuesday, July 13, 2004 7:03 PM
To: [redacted] (OGC) (FBI)
Subject: Sunset Examples

b6
b7C

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

[redacted] - Attached is my final version of the sunset examples. I've incorporated some of the CTD examples. [redacted] NSLB) should be in touch with you tomorrow with additional information on the remainder of the CTD examples. (The SA she needed to speak with was out of the office today.) We found that some of the case examples provided by CTD did not in fact rely upon any of the sunset provisions at all, so they fell out of the analysis. (not unexpectedly)

You will also see that I added two paragraphs addressing the [redacted] case as I mentioned. I do think this bolsters the argument that we need to ensure that 209 does not sunset, especially since we do not have many examples of using this provision.

b2
b6
b7A
b7C

I also added a computer trespasser exception example that involves a hack into the [redacted] computer systems. ([redacted] at [redacted] is my source for almost all the 217 examples). [redacted] was going to check with the [redacted] to ensure that they will not be upset if this is used. I told him that we will assume my current summary is OK unless he contacts you tomorrow.

I think this should be sufficient. However, feel free to contact me if you need anything further. You can reach me either at home or via my cell phone [redacted] over the next two days. I plan to be here on Friday if this is still hanging on by then.

Thanks --

[redacted]

b6
b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
DECLASSIFICATION EXEMPTION 1
~~SECRET//ORCON~~,NOFORN

~~SECRET~~

DATE: 10-21-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 10-21-2030

[redacted] (OGC) (FBI)

CA# 05-CV-0845

b6
b7C

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

From: [redacted] (OGC) (FBI)
Sent: Wednesday, July 14, 2004 1:05 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: Sunset Provisions

DATE: 12-07-2005
CLASSIFIED BY 65179 DHM LP CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-07-2030

~~SECRET~~
RECORD xxxx

[redacted] and [redacted] - I reviewed the summaries for the following cases:

b2
b6
b7A
b7C
b1
b2
b6
b7C
b7E

[redacted] (SSA)
[redacted] (SSA)
[redacted] (SSA)
[redacted] (SSA)
[redacted] (SSA)
[redacted] (SSA)
[redacted] (SSA)

[redacted] (S)

I added information to each one of these summaries (most often at the end) to reflect why the provision was important to the investigation. With respect to [redacted] SSA [redacted] believes that this summary should be deleted as it does not implicate any PATRIOT Act provisions. I have also noted within the document two instances [redacted] and [redacted] in which SSA [redacted] believed that the summaries actually refer to other provisions. We have marked those and noted the more-applicable provisions.

b6
b7A
b7C

If you have any questions, please let me know. Thanks. [redacted]

b6
b7C

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~SECRET~~

~~SECRET~~

DATE: 12-07-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 09-27-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

CA# 05-CV-0845

~~SECRET~~

[redacted] (OGC) (FBI)

From: [redacted] OGC) (FBI) b6
Sent: Thursday, July 15, 2004 12:47 PM b7C
To: [redacted] OGC) (FBI)
Subject: RE: Patriot Act Sunset Provisions: Summary of Field Survey

DATE: 12-07-2005
CLASSIFIED BY 65179 DHM LP CWC
REASON: 1.4 (C)
DECLASSIFY ON: 12-07-2030

b6
b7C

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

[redacted] Met with [redacted] and [redacted] and we finally nailed down which of the CTD examples should be included and which should not. I've listed them below--but I do not know for sure whether you have already included them (since you deleted names, etc, I am not sure in many cases) so, please review and if you have not included them, let's fold them in and we are then ready to send to [redacted] Send to me first and I will comment as I pass them to [redacted]

Section 201 -- nothing ([redacted] was a bust)

Section 203:

[redacted] (S)

b1
b6
b7A
b7C

Section 206 -- Roving FISA -- nothing more than you aready have -- the [redacted] case is out because they never got [redacted]

Section 214

(S) [redacted] think you already have this one in)

(S) [redacted] s out because they got a [redacted]

Section 218

[redacted] (S)

Section 220

~~SECRET~~

~~SECRET~~

[redacted]

b6
b7A
b7C

-----Original Message-----
From: [redacted]OGC) (FBI)
Sent: Friday, July 09, 2004 4:34 PM
To: [redacted](OGC) (FBI)
Subject: Patriot Act Sunset Provisions: Summary of Field Survey

b6
b7C

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

[redacted]- Attached is the draft summary of the field survey we conducted seeking input on the sunset provisions. As you are aware, I am continuing to update this with additional examples provided by CTD.

b6
b7C

[redacted]

Please feel free to contact me if you have any additional questions.

Thanks --

[redacted]

b2
b6
b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~//ORCON,NOFORN

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~//ORCON,NOFORN

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

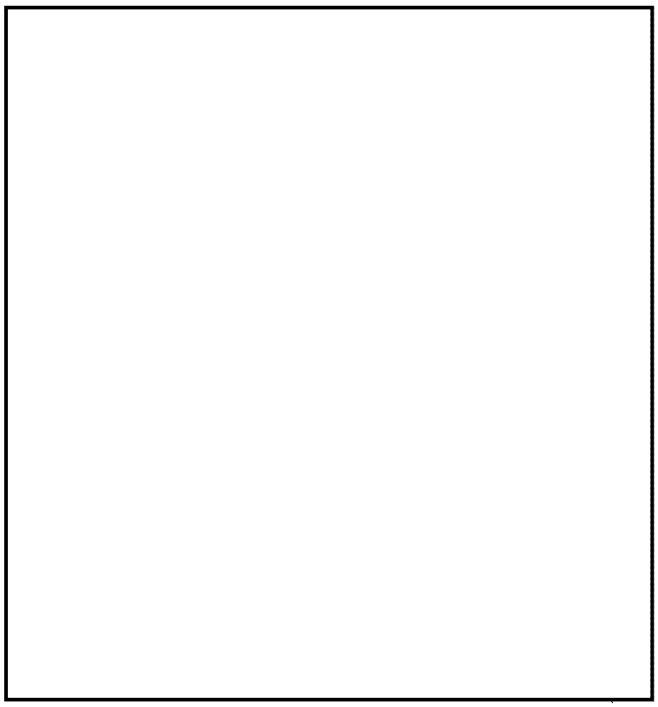
No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 184
Page 5 ~ Duplicate
Page 6 ~ Duplicate
Page 7 ~ Duplicate
Page 8 ~ Duplicate
Page 9 ~ Duplicate
Page 10 ~ Duplicate
Page 11 ~ Duplicate
Page 12 ~ Duplicate
Page 13 ~ Duplicate
Page 14 ~ Duplicate
Page 15 ~ Duplicate
Page 16 ~ Duplicate
Page 17 ~ Duplicate
Page 18 ~ Duplicate
Page 19 ~ Duplicate
Page 20 ~ Duplicate
Page 25 ~ Duplicate
Page 26 ~ Duplicate
Page 27 ~ Duplicate
Page 28 ~ Duplicate
Page 29 ~ Duplicate
Page 30 ~ Duplicate
Page 31 ~ Duplicate
Page 32 ~ Duplicate
Page 33 ~ Duplicate
Page 34 ~ Duplicate
Page 35 ~ Duplicate
Page 36 ~ Duplicate
Page 37 ~ Duplicate
Page 38 ~ Duplicate
Page 39 ~ Duplicate
Page 40 ~ Duplicate
Page 44 ~ b1, b2, b6, b7A, b7C, b7E
Page 45 ~ b1, b2, b6, b7A, b7C, b7E
Page 46 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 47 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 48 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 49 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 50 ~ b1, b2, b6, b7C, b7D, b7E
Page 51 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 52 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 53 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 54 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 55 ~ b1, b2, b6, b7A, b7C, b7D, b7E

Page 56 ~ b1, b2, b6, b7C, b7D, b7E
Page 57 ~ b1, b2, b6, b7C, b7D, b7E
Page 58 ~ b1, b2, b6, b7C, b7D, b7E
Page 59 ~ b1, b2, b6, b7A, b7C, b7E
Page 60 ~ b1, b2, b6, b7A, b7C, b7E
Page 61 ~ b1, b2, b6, b7A, b7C, b7E
Page 62 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 63 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 64 ~ b1, b2, b6, b7A, b7C, b7E
Page 65 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 66 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 74 ~ b2, b7A, b7D, b7E
Page 75 ~ Duplicate
Page 76 ~ Duplicate
Page 77 ~ Duplicate
Page 78 ~ Duplicate
Page 79 ~ Duplicate
Page 80 ~ Duplicate
Page 81 ~ Duplicate
Page 82 ~ Duplicate
Page 83 ~ Duplicate
Page 84 ~ Duplicate
Page 85 ~ Duplicate
Page 86 ~ Duplicate
Page 87 ~ Duplicate
Page 88 ~ Duplicate
Page 89 ~ Duplicate
Page 90 ~ Duplicate
Page 100 ~ Duplicate
Page 103 ~ Duplicate
Page 104 ~ Duplicate
Page 105 ~ Duplicate
Page 106 ~ Duplicate
Page 107 ~ Duplicate
Page 110 ~ Duplicate
Page 111 ~ Duplicate
Page 112 ~ Duplicate
Page 113 ~ Duplicate
Page 117 ~ b1, b2, b6, b7A, b7C, b7E
Page 119 ~ b1, b2, b6, b7A, b7C, b7E
Page 140 ~ Duplicate
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Duplicate
Page 145 ~ Duplicate
Page 146 ~ Duplicate
Page 147 ~ Duplicate
Page 148 ~ Duplicate
Page 149 ~ Duplicate
Page 158 ~ Duplicate

Page 159 ~ Duplicate
Page 160 ~ Duplicate
Page 162 ~ b5
Page 163 ~ b5
Page 164 ~ b1, b5, b6, b7A, b7C
Page 165 ~ b1, b2, b5, b6, b7A, b7C, b7D, b7E
Page 166 ~ b1, b2, b5, b7E
Page 167 ~ b1, b2, b6, b7A, b7C, b7E
Page 168 ~ b1, b2, b5, b6, b7C, b7E
Page 169 ~ b2, b5, b7D, b7E
Page 170 ~ b5, b6, b7A, b7C
Page 171 ~ b1, b2, b5, b7E
Page 172 ~ b1, b2, b5, b7E
Page 173 ~ b1, b2, b5
Page 181 ~ b1, b2, b6, b7A, b7C, b7E
Page 182 ~ b1, b2, b6, b7A, b7C, b7E
Page 183 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 184 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 185 ~ b1, b2, b6, b7A, b7C, b7E
Page 186 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 187 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 188 ~ b1, b2, b6, b7C, b7D, b7E
Page 189 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 190 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 191 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 192 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 193 ~ b1, b2, b6, b7C, b7D, b7E
Page 194 ~ b1, b2, b6, b7C, b7D, b7E
Page 195 ~ b1, b2, b6, b7C, b7D, b7E
Page 196 ~ b1, b2, b6, b7C, b7D, b7E
Page 197 ~ b1, b2, b6, b7A, b7C, b7E
Page 198 ~ b1, b2, b6, b7A, b7C, b7E
Page 199 ~ b1, b2, b6, b7A, b7C, b7E
Page 200 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 201 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 202 ~ b1, b2, b6, b7A, b7C, b7E
Page 203 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 204 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 206 ~ b5
Page 207 ~ b5
Page 208 ~ b1, b5, b6, b7A, b7C
Page 209 ~ b1, b2, b5, b6, b7A, b7C, b7D, b7E
Page 210 ~ b1, b2, b5, b6, b7A, b7C, b7D, b7E
Page 211 ~ b2, b6, b7A, b7C, b7E
Page 212 ~ b1, b2, b5, b6, b7A, b7C, b7E
Page 213 ~ b2, b5, b7E
Page 214 ~ b2, b5, b7D, b7E
Page 215 ~ b5, b6, b7A, b7C
Page 216 ~ b1, b2, b5, b7E
Page 217 ~ b1, b2, b5, b7E
Page 218 ~ b1, b2, b5

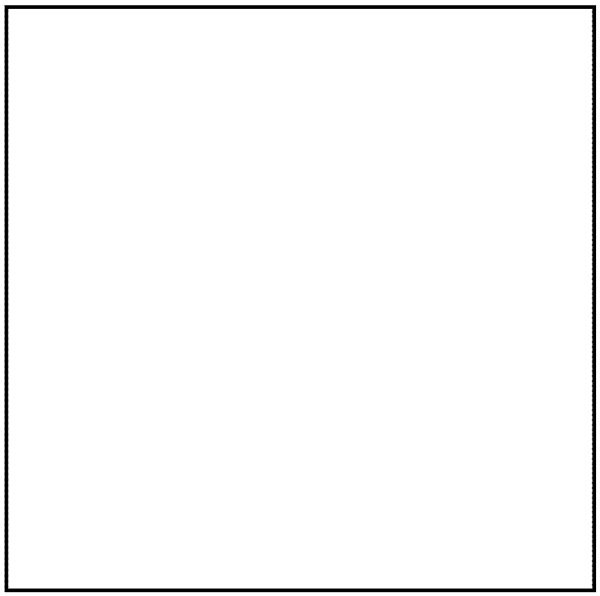
Page 239 ~ b5
Page 240 ~ b5
Page 241 ~ b1, b5, b6, b7A, b7C
Page 242 ~ b1, b2, b5, b6, b7A, b7C, b7D, b7E
Page 243 ~ b1, b2, b5, b6, b7C, b7E
Page 244 ~ b2, b5, b7A, b7E
Page 245 ~ b1, b2, b5, b6, b7A, b7C, b7E
Page 246 ~ b1, b2, b5, b6, b7C, b7E
Page 247 ~ b1, b2, b5, b7E
Page 248 ~ b2, b5, b7D, b7E
Page 249 ~ b5, b6, b7A, b7C
Page 250 ~ b5, b7A
Page 251 ~ b1, b2, b5, b7E
Page 252 ~ b1, b2, b5
Page 253 ~ b2, b5, b7E
Page 255 ~ b1, b2, b6, b7A, b7C, b7E
Page 256 ~ b1, b2, b6, b7A, b7C, b7E
Page 257 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 258 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 259 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 260 ~ b1, b2, b5, b6, b7A, b7C, b7D, b7E
Page 261 ~ b1, b2, b6, b7C, b7D, b7E
Page 262 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 263 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 264 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 265 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 266 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 267 ~ b1, b2, b6, b7C, b7D, b7E
Page 268 ~ b1, b2, b6, b7C, b7D, b7E
Page 269 ~ b1, b2, b6, b7C, b7D, b7E
Page 270 ~ b1, b2, b6, b7A, b7C, b7E
Page 271 ~ b1, b2, b6, b7A, b7C, b7E
Page 272 ~ b1, b2, b6, b7A, b7C, b7E
Page 273 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 274 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 275 ~ b1, b2, b6, b7A, b7C, b7E
Page 276 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 277 ~ b1, b2, b6, b7A, b7C, b7D, b7E



b5

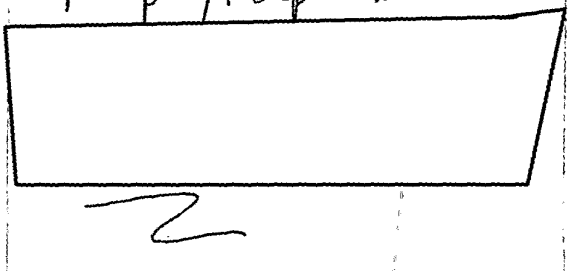
§207 - extended duration of FISAs.

- allows FBI/DOJ personnel to spend time on new FISAs rather than renewals.



b5
b6
b7C

Sounds like we got location tracking info w/ a pen/trap order.



b5

b6
b7C

From [redacted] *presentation*

Patriot Act Overview

I. Substantive Criminal Offense:

A. **Deterrence and Prevention of Cyberterrorism**: 18 U.S.C. § 1030, Computer Fraud and Abuse Act.

1. makes explicit that a hacker need only intend damage, not a particular *type* of consequence or degree of damage;
2. adds a new offense for damaging computers used for national security or criminal justice (a)(5)(B);
3. makes explicit that the definition of "protected computer" includes computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce--so foreigner hacking through a U.S. computer violates 1030--allows US to assist in international hacker investigation or gives US option of prosecuting such criminals int he U.S.;
4. allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold under (a)(5)(B).
5. Adds definition of "loss" as including "any reasonable cost to any victim..."
6. increases penalties for hackers who damage protected computers (from a maximum of 10 years for first offenders & a maximum of 20 years for repeat offenders) also eliminated mandatory minimum;
7. counts state convictions as "prior offenses" for purpose of recidivist sentencing enhancements

II. Investigative Tools: Most provisions will sunset December 31, 2005.

A. **Predicate Offenses**: Amends 18 U.S.C. § 2516(1): adding felony violations of 18 U.S.C. § 1030 to the list of predicate offenses,[1] authorizing wiretap order to intercept *wire* communications (those involving the human voice). Also adds Terrorism offenses as predicate offenses.

B. **Obtaining Voice-mail and Other Stored Voice Communications:** stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order).

C. **Scope of Subpoenas for Electronic Evidence**: expands list of "basic subscriber" records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Moreover, the amendments clarify that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for his or her account with a communications provider, "including any credit card or bank account number.

D. **Emergency Disclosures by Communications Providers**:

1. amends subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not

[1] This amendment does not affect applications to intercept *electronic* communications in hacking investigations. As before, investigators may base an application to intercept electronic communications on any federal felony criminal violation. 18 U.S.C. § 2516(3).

create an affirmative obligation to review customer communications in search of such imminent dangers.

2. clarifies that service providers *do* have the statutory authority to disclose non-content records to protect their rights and property. (subsection 2702(c)(3)).

E. **Intercepting the Communications of Computer Trespassers**

1. allows victims of computer attacks to authorize persons "acting under color of law" to intercept the communications of a computer trespasser transmitted to, through, or from a protected computer.[2] Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.
2. Four requirements must be met before monitoring can occur:
   a. the owner or operator of the protected computer must authorize the interception of the trespasser's communications.
   b. the person who intercepts the communication must be lawfully engaged in an ongoing investigation.
   c. the person acting under color of law must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation.
   d. investigators are permitted to intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.
3. Anticipate further DOJ/FBI guidance on procedures to document "consent"

F. **Nationwide Search Warrants for Stored Communications:**

1. allows investigators to use section 2703(a) warrants to compel records outside of the district in which the court is located, just as they use federal grand jury subpoenas and orders under section 2703(d).
2. This change enables courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major ISPs are located.

G. **Authority for Delaying Notice of the Execution of a Warrant**

1. amending 18 U.S.C. § 3103a to create a uniform statutory standard authorizing courts to delay the provision of required notice if the court finds "reasonable cause" to believe that providing immediate notification of the execution of the warrant may have an adverse result as defined by 18 U.S.C. § 2705 (including endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation or unduly delaying a trial). The section provides for the giving of notice within a "reasonable period" of a warrant's execution, which period can be further extended by a court for good cause.
2. the Department may be providing additional guidance with respect to the use of this delayed notice provision. The Department expects that delayed notice will continue to be an infrequent exception to the general rule that notice of the execution of a warrant will be provided promptly.

H. **Clarifying the Scope of the Cable Act:** amends title 47, section 551(c)(2)(D), to clarify that ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services – such as telephone and Internet services. The amendment preserves, however, the Cable Act's primacy with respect to records revealing what ordinary cable television programing a customer

---

[2] "computer trespasser" is defined to include any person who accesses a protected computer (as defined in section 1030 of title 18) without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21).

J. **National Security:** all provisions below will sunset in December 2005

1. Foreign Intelligence Information: amends 50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B) to permit FISA surveillance and search requests if they are for a "significant" intelligent gathering purpose, rather than "the" purpose. Suggests a recognition that parallel intelligence and criminal investigations may occur on the same target.

2. Roving Surveillance: expands FISA court orders to allow "roving" surveillance similar to Title III.

3. Duration of FISA surveillance: for electronic surveillance, the initial period authorized for 120 days (from 90 days) and extensions from 90 days to one year. For physical searches, the initial period authorized for 90 days (from 45).

4. Pen Register and Trap and Trade Authority under FISA: allows order based only on certification that the information obtained would be relevant to an on-going intelligence investigation when it is for the protection against international terrorism or clandestine intelligence activities, provided that investigations of U.S. persons is not based solely on First Amendment activities.

5. Access to Records and Other Items under FISA: Requires a FISA court order to obtain business records; allows any FBI designee no lower than Assistant Special Agent in Charge to apply to FISA court for ex parte order; limits the use of this authority to investigations to protect against international terrorism or clandestine intelligence activities; investigations of U.S. persons may not be based solely on First Amendment activities.

III. Information Sharing and Other Provisions

A. Authority to share criminal investigative information.

1. Grand Jury Information: Allows intelligence or counterintelligence or foreign intelligence information obtained in grand jury proceedings or otherwise as part of a criminal investigation to be shared with any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

   a. Requires 6(e) notification to court after disclosure stating the fact that such information was disclosed and the departments, agencies, or entities to which disclosure was made.

2. Title III Information: Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties.

3. Foreign Intelligence Information: Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties.

4. Recipient may use the information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

5. *Attorney General must establish procedures for the disclosure of information pursuant to Title III and Rule (6)(e) that identifies a U.S. person.*

6. Requires the Attorney General to disclose to the CIA Director foreign intelligence acquired by the Justice Department in the course of a criminal investigation, except when disclosing such information would jeopardize an ongoing investigation.

B. Secret Service Jurisdiction: Amends 18 U.S.C. 1030(d)(1):

1. The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under the Computer Fraud and Abuse Act.
2. The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.
3. Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

C. Expansion of National Electronic Crime Task Force Initiative.

1. Directs the Secret Service to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

D. Development & Support of Cybersecurity Forensic Capabilities: Requires the Attorney General to establish regional computer forensic laboratories.

December 28, 2001
C:\WINDOWS\TEMP\PATRIOTA.WPD

See Red Flag -
Is this DAG Memo
the one [redacted]
Issued EC on?
If so, read +
put copy in
ELSUR notebook.

b6
b7C

Sensenbrenner Letter

April 1, 2003

The Honorable John D. Ashcroft
Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Attorney General Ashcroft:

As the Chairman and Ranking Member of the House Committee on the Judiciary, it is our responsibility to conduct oversight of the Department of Justice's efforts to combat terrorism, which includes implementation of the USA PATRIOT Act ("Act") signed into law by President Bush on October 26, 2001. In response to our letter of June 13, 2002, you provided us with information regarding the use of these new tools, which helped us to understand the complexity and extensive scope of the effort to implement the law.

The Department of Justice has also been faced with significant new challenges to which it has responded using existing authorities as well as those contained in the Act. This letter seeks information regarding the use of preexisting authorities and the new authorities conferred by the Act.

Unless otherwise indicated, please provide your responses to the Committee current through March 31, 2003. In addition, if any answer requires the disclosure of classified material, please provide those answers under separate cover to the Committee or to the House Permanent Select Committee on Intelligence ("HPSCI") in accordance with appropriate security procedures. We will review those responses under appropriate procedures that HPSCI and this Committee establish pursuant to the rules of the House.

To the extent that a question relates to the authority or operations of the Immigration and Naturalization Service, all of which have been transferred to the Department of Homeland Security ("DHS"), you may either answer the question or refer the questions to the appropriate official at DHS. If you refer the question to DHS, please notify us of the identity of the official to whom the question has been referred.

Please respond to the following questions:

USA PATRIOT Act

1. Section 215 of the Act amended 50 U.S.C. § 1861 to allow the FBI Director or his designee (who must hold the rank of Assistant Special Agent in Charge or higher) to apply for an order from the Foreign Intelligence Surveillance Court for "the production of tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities . . . ." Such an investigation may only be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order). 50 U.S.C. § 1861(a)(2)(A).

   A. What guidelines has the Attorney General approved under Executive Order 12333 or a successor order for the conduct of such investigations?

   B. Before such an order can be sought, do the guidelines require that the FBI have already established

probable cause that a person under investigation is an agent of a foreign power? What is the Department's definition of "probable cause" and how has it changed since September 11, 2001?

C. Please produce all guidelines approved under Executive Order 12333 or a successor order for the conduct of such investigations.

2. Such investigations also may not be conducted of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. § 1861(a)(2)(B). Other authorities under the Foreign Intelligence Surveillance Act ("FISA") are also subject to the limitation that an investigation of a United States person in which those authorities are used may not be conducted solely on the basis of activities protested by the First Amendment to the U.S. Constitution. See, e.g., 50 U.S.C. § 1842 (regarding pen register and trap and trace orders under FISA).

A. In seeking such orders, does the government make an explicit certification that an investigation of a United States person is not being conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States?

B. In issuing such orders, does the court make an express finding that an investigation of a United States person is not being conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States?

3. The Department has increased the use of "national security letters" that require businesses to turn over electronic records about finances, telephone calls, e-mail and other personal information.

A. Please identify the specific authority relied on for issuing these letters.

B. Has any litigation resulted from the issuance of these letters (i.e. challenging the propriety of legality of their use)? If so, please describe.

4. Has any administrative disciplinary proceeding or civil action been initiated under section 223 of the Act for any unauthorized disclosure of certain intercepts? If so, please describe each case, the nature of the allegations, and the current status of each case.

5. In the Administration's 2004 Budget Request, DOJ is requesting $22 million to establish an automated cross-case analytical system to facilitate sharing case specific information through the agencies that belong to the Organized Crime Drug Enforcement Task Force Program. These include law enforcement agencies in DOJ, the Department of Homeland Security, and the Department of Treasury. Is this system also intended to facilitate implementation of the authority to share criminal investigative information with intelligence officials under Section 203 of the Act? Will it be used for that purpose?

6. What has been the role of the Department in establishing standards or procedures regarding implementation of the authorities provided in Section 358 (Bank Secrecy Provisions and Activities of United States Intelligence Agencies to Fight International Terrorism)? Please provide any written guidance regarding the requirements of that section that the Department has either issued or approved.

7. What are the dollar amounts that have been paid under the reward authorities provided in Section 501 of the Act or the terrorism related awards under the newly enacted 28 U.S.C. § 530(C)(b)(1)(J)? How many non-U.S. citizens have received rewards under these authorities?

8. The Administration's Office of Justice Programs 2004 Budget request includes a $12 million increase for Regional Information Sharing System (RISS) improvements. The request refers to Section 701 of the USA PATRIOT Act

and states that the requested increase will be used to expand RISS's accessibility to state and local public safety agencies to share terrorism alerts and related information. Please provide the Committee with a description of the management oversight process by which DOJ will ensure that the proposed expenditures will accomplish improvements in the U.S. information infrastructure and the specific improvements that are envisioned. Please provide copies of any guidance issued to state and local agencies with respect to the further dissemination of such materials.

9. Under section 213 of the USA PATRIOT Act, a court may order a delay in any notice of the execution of a search warrant if "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result," which is defined as (1) endangering the life or physical safety of an individual; (2) flight from prosecution; destruction or tampering with evidence; (3) intimidation of potential witnesses; or (4) otherwise seriously jeopardizing an investigation or unduly delaying trial. Please respond to the following questions regarding the use of this authority:

   A. How many times has the Department of Justice sought an order delaying notice of the execution of a warrant under this section?

   B. How many times has a court ordered the delay in such notification?

10. That same section allows the notice to be delayed when the warrant prohibits the seizure of among other things, any tangible property, unless "the court finds reasonable necessity for the seizure." 18 U.S.C. § 3103a (b)(2).

   A. Since the enactment of that section, how many times has the government asked a court to find reasonable necessity for a seizure in connection with delayed notification under this section?

   B. On what grounds has the government argued that seizure was reasonably necessary under a warrant for which the government also asked for delayed notification?

   C. How often has a court found "reasonable necessity for the seizure" in connection with a warrant for which it also permitted delayed notification?

   D. How often has a court rejected the government's argument that a seizure was reasonably necessary in connection with a warrant for which the government sought delayed notification?

   E. On what grounds have the courts found that the seizures were reasonably necessary in connection with warrants for which delays in notification were granted?

   F. What grounds have the courts rejected as establishing reasonable necessity for a seizure in connection with a warrant for which the government sought delayed notification?

11. That same section allows a court to order delayed notice when "the warrant provides for the giving of such notice within a reasonable period of its execution, which may be extended for by the court for good cause show." 18 U.S.C. § 3103a(b)(3).

   A. What are the shortest and longest periods of time for which the government has requested initial delayed notice?

B. On what grounds has the government argued that the period of delayed notification was reasonable?

C. How often has the government sought an extension of the period of delayed notice?

D. On what grounds has the government asked for an extension of the period of delayed notice?

E. How often has a court rejected the government's request for delayed notification on the ground that the period for giving delayed notice was unreasonable?

F. On what grounds have the courts rejected the government's position that the period for giving delayed notice was reasonable?

G. How often has a court rejected the government's request for an extension of the period of delayed notification?

H. On what grounds have the courts rejected the government's argument that an extension of the period for delayed notice was reasonable?

12. On January 21, 2003, the *Wall Street Journal* published an article entitled "New Powers Fuel Legal Assault on Suspected Terrorists." That article claims that the Department of Justice is using information that was "previously largely unavailable" and that had been obtained from FISA surveillance to support criminal prosecutions. According to the article, this information is now available to prosecutors as a result of the FISA Review Court's decision regarding the meaning of the Act's amendment to FISA permitting the government to obtain a surveillance order when "a significant purpose," (rather than "the purpose") of the surveillance is to collect foreign intelligence.

A. Prior to the FISA Review Court's decision, as long as surveillance was properly ordered for "the purpose" of collecting foreign intelligence, was there any legal impediment to prosecution of a crime using evidence obtained under FISA?

B. Please identify all cases brought since the FISA Review Court's decision that use information that was previously unavailable under FISA procedures.

C. Please explain why such information was unavailable and why it became available following the FISA Review Court's decision.

13. The FISA Review Court's decision permits enhanced coordination between law enforcement and intelligence officials.

A. What FISA-related training is currently being planned or conducted?

B. What topics will it address?

C. Who will give the training?

D. Who will receive the training?

E. Is the training going to be coordinated with the Intelligence Community in general and/or the Director of Central Intelligence?

14. How many emergency FISA surveillance orders did the Department of Justice process between FISA's enactment and September 11, 2001? How many has it processed since September 11, 2001? Has the change from 24 to 72 hours in 50 U.S.C. 1805(f) and 1824(e) facilitated the use of FISA emergency searches and surveillance, and if so, how?

15. Since enactment of the USA Patriot Act, what procedures have been implemented to improve the efficiency of processing FISA applications?

16. In testimony presented to the Senate Judiciary on March 4, 2003, FBI Director Robert Mueller stated that:

> The FBI's efforts to identify and dismantle terrorist networks have yielded major successes over the past 18 months. We have charged over 200 suspected terrorists with crimes - half of whom have been convicted to date. The rest are awaiting trial. Moreover, our efforts have damaged terrorist networks and disrupted terrorist plots across the country. In the past month alone, the FBI has arrested 36 international and 14 domestic suspected terrorists.

A. What authorities under the USA PATRIOT Act were used in identifying and dismantling terror networks and were relied upon to prevent terrorist plots?

B. In your judgment, how many of those investigations would have been much more difficult or impossible without the authorities available under the Act?

17. The Act supplemented the government's authority to freeze and forfeit assets of suspected terrorists and terrorist organizations. Please provide the Committee with information related to the freezing or confiscation of such assets since the enactment of the Act.

A. Please identify all suspected terrorists or terrorist organizations whose assets the federal government has frozen or forfeited?

B. Please identify the specific authority, whether or not under the Act, that the federal government has asserted in freezing or forfeiting the assets of suspected terrorists or terrorist organizations.

C. Have any seizures or forfeitures been challenged in court?

D. What have been the results of any such challenges?

E. Has any court, pursuant to section 316 of the Act (codified at 18 U.S.C. § 983 note), admitted evidence that would otherwise be inadmissible in a forfeiture proceeding? If so, on what circumstances justified admitting such evidence in such cases?

18. Section 402 authorizes appropriations to triple the number of INS Border Patrol Agents and Inspectors in each state along the Northern Border, and also authorizes appropriations to provide necessary personnel and facilities to support such personnel.

A. How many additional Inspectors has the INS hired at the Ports of Entry along the Northern Border?

B. How many of those hires are working as Inspectors along the Northern Border at this time?

C. By how many Inspectors has the total staffing at the ports along the Northern Border increased since September 11, 2001?

19. What technology improvements have been completed and what additional technology improvements are planned for FY2003 expenditures to improve Northern Border security?

20. Subtitle B of Title IV of the USA PATRIOT Act gives the Attorney General additional authority to detain certain suspected alien terrorists, and improves systems for tracking aliens entering and leaving the United States and for inspecting aliens seeking to enter the United States. Section 411 amends the Immigration and Nationality Act (INA) to broaden the scope of aliens ineligible for admission or deportable due to terrorist activities, and defines the terms "terrorist organization" and "engage in terrorist activity."

A. Has the INS relied upon the definitions in section 411 of the Act to file any new charges against aliens in removal proceedings? If so, how many times has it used each provision?

B. In your July 26, 2002 response, you stated that one alien had been denied admission under these new provisions. Have any aliens been denied admission under these grounds since that response?

C. What effect have the amendments to the INA in section 411 of the Act had on ongoing investigations in the United States?

D. Section 212(a)(3)(F) of the INA, as amended by section 411 of the Act, renders inadmissible any alien who the Attorney General determines has been associated with a terrorist organization and intends while in the United States to engage solely, principally, or incidentally in activities endangering the United States. Has the Attorney General made such a determination with respect to any alien thus far?

E. Have there been any challenges to the constitutionality of the charges added to the INA by section 411 of the Act? If so, please identify the case(s) and the status of the proceedings.

21. Section 412 of the Act provides for mandatory detention until removal from the United States (regardless of relief from removal) of an alien certified by the Attorney General as a suspected terrorist or threat to national security. It also requires release of such alien after seven days if removal proceedings have not commenced, or if the alien has not been charged with a criminal offense. In addition, this section of the Act authorizes detention for additional periods of up to six months of an alien not likely to be deported in the reasonably foreseeable future if release will threaten our national security or the safety of the community or any person. It also limits judicial review to habeas corpus proceedings in the U.S. Supreme Court, the U.S. Court of Appeals for the District of Columbia, or any district court with jurisdiction to entertain a habeas corpus petition, and limits the venue of appeal of any final order by a circuit or district judge under section 236A of the INA to the U.S. Court of Appeals for the District of Columbia.

A. At the time of your July 26, 2002 response, you had not used the authority in Section 412. Have you used the authority since that response? If so, please state:

i. How many of the aliens for whom certifications have been issued have been removed?

ii. How many aliens for whom the Attorney General issued certifications are still detained? At what stage of the criminal or immigration proceedings are each of those cases?

iii. How many of the aliens who were certified have been granted relief? How many of those aliens are still detained?

iv. Have any challenges to certifications under section 236A(a)(3) of the INA been brought in habeas corpus proceedings in accordance with section 236A(b)? If so, please identify the case(s) and the status of each proceeding.

v. Has the Attorney General released any aliens detained under section 236A because the alien was not charged with a criminal offense or placed into removal proceedings within seven days?

vi. How many non-certified aliens have received relief from removal and remain detained longer than 6 months since such relief was ordered?

22. On September 20, 2001, the INS issued an interim rule amending the period of time that an alien may be detained while the agency assesses whether to issue a Notice to Appear (NTA), placing the alien in immigration proceedings. Prior to amendment, the INS was required to issue an NTA within 24 hours of the alien's arrest. As amended, the INS has 48 hours after an alien is arrested to decide whether to issue an NTA, "except in the event of an emergency or other extraordinary circumstance in which case a determination will be made within an additional reasonable period of time."

A. What is the authority for the INS to detain an alien for longer than 48 hours without filing charges?

B. How many aliens have been detained for more than 48 hours without being charged under the authority in this regulation?

C. What is the longest period that an alien has been detained without being charged under the authority in this regulation?

D. Have any challenges to this regulation been brought in judicial proceedings? If so, please identify the case (s) and the status of each proceeding.

23. Since September 11, 2001, the government has required that certain non-citizens from certain Middle Eastern countries register with the INS (or its successor agency).

A. How many terrorists or suspected terrorists have been investigated and/or detained as a result of the requirement that non-citizens register with the federal government?

B. What is the government's policy regarding whether non-citizens are able to have counsel present during the registration process, specifically during the interview?

C. If counsel are not permitted at any point, what is the government's authority for denying such right to counsel?

24. Since September 11, 2001, how many individuals have been deported from the United States? To what countries were those individuals deported? What was the racial and ethnic background of such individuals? For what reason were these individuals deported?

Attorney General's Investigative Guidelines

25. On May 14, 2002, the Department issued revised investigative guidelines that established procedures for the initiation of investigations by the Federal Bureau of Investigation ("Bureau").

A. Why were the guidelines for General Crimes and Domestic Security Investigations revised when the apparent threat against the United States is a threat from foreign terrorist groups? Do these guidelines apply only to investigations of U.S. citizens? Are U.S. citizens not subject to the foreign intelligence investigative guidelines?

B. The new guidelines allow FBI agents to attend a public event, such as a political demonstration or a religious service, and to use data mining services, provided doing so is for the purpose of preventing or detecting terrorism. How will it be determined that the purpose of attending the event or using the service is to prevent or detect terrorism? How does the amount of evidence establishing that predicate differ from the amount of evidence that would be sufficient to check out leads or open a preliminary inquiry? What level of predication is required to permit FBI agents to attend public events or to use data mining services?

C. Since the issuance of these guidelines, how many religious sites (mosques, churches, temples, synagogues, etc.) have federal authorities entered in an official capacity without disclosing their identities? Please provide the total number of such sites and a breakdown of how many were affiliated with each particular type of site (mosque, church, temple, synagogue, etc.).

When agents visit religious sites pursuant to AG guidelines, what investigative tools are they permitted to use (i.e., wearing a wire, placing a listening device in the site)? If the information obtained from such visits is found unrelated to any criminal or terrorist investigation, when is such information destroyed and in what manner? Have, and if so provide details, any terrorism-related investigations or prosecutions resulted from such visits?

D. Since the issuance of these guidelines, how many public meetings, and what types of such meetings (rallies, town halls), have federal authorities entered in an official capacity without disclosing their identities?

When agents visit public meetings pursuant to FBI guidelines, what investigative tools are they permitted to use (e.g., wearing a wire, placing a listening device in the meeting area)? If the information obtained from such visits is found unrelated to any criminal or terrorist investigation, when is such information destroyed and in what manner? Have, and if so provide details, any terrorism-related investigations of prosecutions resulted from such visits?

E. Are FBI agents required to record in writing – before they use data mining techniques or attend a public event under the guidelines -- how such activity is for the purpose of detecting or preventing terrorism?

F. The changes to the preliminary inquiry procedures extended the period that such an inquiry can remain open and allowed extensions for up to a year without notice to FBI Headquarters. In considering this change, did you find that your field agents had been reluctant to conduct preliminary inquiries because they could not keep them open long enough without burdensome approval requirements? What other problems did the 90-day limit present to agents? What other problems did requiring approval from Headquarters to continue a preliminary inquiry present to agents? How does Headquarters conduct important analysis of

information generated by a preliminary inquiry if Headquarters is unaware of the inquiry for a year?

G. The Guidelines now permit a Special Agent in Charge to open a terrorism enterprise investigation without obtaining approval from FBI Headquarters. Instead, Headquarters must only be notified. What is contained in the required notice? Does the notice provide enough of a description of the evidence to permit FBI Headquarters to make an evaluation of the evidence and determine whether the investigation should continue or is it simply a formal notification that such an investigation has been opened and/or is continuing? Will the information in the notification be sufficient to use it to coordinate that investigation with others?

H. Who at the Bureau is responsible for making and approving the decision for a field agent to enter a public place, and must such approval be in writing prior to entering the public place?

I. After a field agent visits a public place or event, are any notes or other records of what he or she observed retained? If so, under what circumstances, for what reasons, and for how long are they retained? Under what circumstances is information related to protected 1st Amendment activity retained in FBI or DOJ files? Are any records retained if a preliminary inquiry is never opened?

J. Who has access to any records and how does the FBI keep them secure?

K. Given the transfer of a substantial number of agents into terrorism investigations, what training did those agents receive on the use of the Guidelines?

L. With the FBI's authority to "data mine" under the Guidelines, many fear that the FBI will have too much information and that the Bureau does not currently have the tools necessary to make good use of intelligence or to keep vast amounts of information secure. What has been done and is being done to improve the Bureau's ability to interpret all of this new data? What security measures have been implemented to prevent unauthorized access to such data?

M. Since the Guidelines permit the use of "publicly available" information, what efforts are going to be made to verify the accuracy of the data retrieved? Will agents be required to attempt to independently verify retrieved information for accuracy?

N. What type of supervision will be required when agents use data mining? Will field agents be able to initiate data mining on their own or will they be required to obtain approval from a supervisor?

O. What data mining services has the FBI used? How long will data obtained through data mining be retained and how will it be indexed?

P. In its May 2002 Report on Financial Privacy, Law Enforcement, and Terrorism, the Prosperity Task Force on Information Exchange and Financial Privacy outlined many problems with sharing too much information with too many countries and without proper controls. How has the FBI protected against the wide distribution of information to too many countries without proper controls?

Q. Since Syria, Cuba, Libya, Iran, Iraq, China, and others are members of Interpol and share in the international information exchange system, what procedures prevent these countries from receiving information on terrorist suspects who may be supported by participating countries?

R. The Guidelines permit acceptance and retention of information "voluntarily provided by private entities."

What will the FBI do to ensure the accuracy of the information received from such sources? To what extent have such "private entities" been third parties as opposed to the specific individuals to whom the information pertained? How does the Department interpret "voluntarily" (e.g., does it mean the information was unsolicited, was provided pursuant to a government request, or was provided pursuant to a government subpoena?)?

S. Where and how is information obtained through data mining stored? Is access to data obtained through data mining limited to those involved in a particular investigation? How is erroneous information corrected or purged, if at all? Has the Department issued written policies to provide guidance in this area? Does it plan to issue such policies?

Has, and from what companies, the Department purchased information or entered into contracts with data mining companies? To what extent and how will persons listed in such information be able to correct errors or inaccuracies?

T. Is retained information reviewed at reasonable intervals to determine its continuing relevance to antiterrorism efforts? If so, who is responsible for performing such reviews?

Miscellaneous Authorities

26. There have been numerous reports that the Department of Justice has detained individuals as material witnesses, presumably pursuant to judicial orders under 18 U.S.C. § 3144, in connection with terrorism investigations. Please provide the Committee with the following information with respect to each such detainee since September 11, 2001: (1) the length of detention of each detainee; (2) the number of such detainees who either sought review of or filed an appeal from a detention order under 18 U.S.C. § 3145; and (3) the results of such review or appeal.

A. Were these individuals given access to legal counsel? If not, why not?

B. What is the percentage breakdown for the detainees in terms of national origin, race, and ethnicity?

C. Please list the charges that the Department has brought against each such detainee.

D. Please provide the legal basis for detaining those individuals who have been cleared of any connection with terrorism beyond the date of such clearance.

E. Please provide a list of all requests by the government to seal proceedings in connection with any of the detainees and copies of any orders issued pursuant thereto.

27. On October 31, 2001, the Department of Justice promulgated an interim rule, with provision for post promulgation public comment, that requires the director of the Bureau of Prisons to monitor or review the communications between certain inmates and their lawyers for the purpose of deterring future acts that could result in death or serious bodily injury to persons or substantial damage to property that would entail the risk of death or serious bodily injury to persons. 66 Fed. Reg. 55062, 55066 (2001).

A. How many inmates have been subject to the interim rule?

B. The interim rule required prior written notification to an inmate and any attorneys involved "[e]xcept in the case of prior court authorization. 66 Fed. Reg. at 55066. Under this exception to the required notification, how many cases were there/are there where inmates and their attorneys were not notified that their communications were monitored?

C. The interim rule prohibited disclosure of information prior to approval of disclosure by a federal judge, except where the person in charge of the monitoring determines that acts of violence or terrorism are imminent. How many times did the person in charge of the monitoring disclose information after approval by a federal judge? After a determination that acts of violence or terrorism are imminent?

D. How many post-promulgation comments were received by the Department of Justice?

E. Is the Department of Justice considering any revisions to the interim rule?

28. The Department of Defense has detained two United States citizens in military prisons in the United States as enemy combatants. These detentions have been challenged in court, where the Department of Justice has represented the Department of Defense. Has the Department of Justice received any information regarding the detention by the Department of Defense within the United States or abroad of any other United States citizens? Does the Department of Justice have any agreement, arrangement, or understanding, formal or informal, with the Department of Defense regarding the detention of United States citizens as enemy combatants?

29. FBI Director Robert Mueller announced the formation of "flying squads" that would be prepared to be deployed on short notice into terrorism investigations.

A. Have these "flying squads" been formed?

B. How many agents are assigned to a flying squad?

C. What kind of training have the flying squad agents received?

D. Have they been deployed into investigations?

E. If so, how many times?

F. Did they prove to be a useful addition to the investigation to which they were deployed?

30. Does the FBI use, as one of its terrorism investigative tools, aircraft to conduct surveillance of various persons or locations? What type of information is sought using such surveillance?

31. Has the DOJ through any of its agencies formulated a policy position regarding criteria for establishing the authenticity of foreign government-issued identity cards since the passage of the USA PATRIOT Act? If so, please produce a copy of that position.

32. Has the DOJ through any of its agencies, including especially the INS, prepared or issued a policy with regard to security standards and acceptance of "Matricula Consulars" identity cards issued by foreign governments to persons who are residing in the United States but who may not be lawfully present in the United States.? If so, has that policy been provided in writing to the Office of Management and Budget, the Secretary of State, or the Secretary of the Treasury? If such a policy has been prepared, please provide a copy to the Committee.

33. Regarding the FBI's National Crime Information Database, has the Department lifted a requirement that the FBI ensure the accuracy and timeliness of information about criminals and crime victims before adding it to the

database? Please provide a copy of any memoranda pertaining to the requirement that was lifted.

34. Is the FBI is ordering its field offices to ascertain the number of mosques and Muslims in their areas? Is the government seeking membership lists from mosques? If so, why? From how many mosques is the government seeking such lists? How, if at all, has the agency reassigned its agents as a result? How many investigations of or prosecutions for terrorism as a result of these activities?

35. Is the Department assisting in the implementation of the Computer Assisted Passenger Prescreening System (CAPPS I or II), which would be used to screen airline passengers?

    A. To what extent is the Department, or any of its components, providing information about specific persons for inclusion in CAPPS?

    B. From what databases or other sources, including companies, does such information come from?

    C. What checks are in place to ensure that the information is accurate and does not constitute inappropriate profiling?

    D. In what manner are individuals afforded an opportunity to correct erroneous or inaccurate information?

36. "Operation Liberty Shield" involves stopping cars at airports, checking the identification of truckers who transport hazardous material on the highway, and monitoring Internet and financial transactions.

    A. Please identify the specific authority on which "Operation Liberty Shield" was created and implemented.

    B. What level of predication is required before an agent may monitor the Internet and financial transactions?

    C. What terrorism-related investigations and/or prosecutions have resulted from Operation Liberty Shield?

37. There have been three successive FBI sweeps since September 11, 2001, to monitor, question, arrest, detain, or deport various immigrants. The first sweep focused on young Arab and Muslim males and occurred in the months following September 11, 2001. The second sweep occurred in March 2002 and centered on thousands of individuals of Middle Eastern and South Asian heritage. The third sweep occurred in March 2003 as part of "Operation Liberty Shield." Please provide information on each of these operations.

    A. When were the plans for such operations first considered by the Department?

    B. What guidance was provided to U.S. Attorney's Offices and/or FBI offices with respect to questions that should be asked of such immigrants?

    C. What has been the outcome of each of these plans? Please provide details such as how many were monitored, questioned, arrested, detained, or deported for each operation. Please provide details as to the number and types of terrorism-related investigations and prosecutions that have resulted from these sweeps.

    D. Please identify the specific authority relied on to create and implement these plans, including the monitoring, questioning, arrests, detentions, and deportations.

38. In August 2002, a Justice Department rule went into effect giving authority to state and local police to enforce

immigration laws.

A. Which state and local governments are using this new authority and to what extent?

B. How many immigration violations were found as a result of state and local law enforcement participation under this new authority?

C. Have any persons or groups affected by this new authority (e.g. immigrants, civil rights organizations) submitted any formal complaints to the Department (including the Inspector General) regarding this authority. If so, please provide details.

Please forward your responses to these questions to the Committee at the address on this letter not later than Tuesday, May 13, 2003. Please contact Committee Chief of Staff and General Counsel Phil Kiko at 202-225-3951 or Minority Counsel Sampak Garg at 202-225-6906 if you have any questions about this request.

Sincerely,

F. JAMES SENSENBRENNER, JR.
Chairman

JOHN CONYERS, JR.
Ranking Member

FJS/pgk

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

DRAFT

Precedence: ROUTINE **Date:** ~~12/19/2001~~ 1/18/2002

To: Laboratory

All Field Offices

Attn: All ITB Section Chiefs
All ITB Unit Chiefs
All ITB Supervisory Special Ag
Technical Supervisors
Technical Advisors
Chief Division Counsel (for information)

From: Laboratory
Investigative Technologies Branch
and
Office of the General Counsel

Contact: [redacted]

Approved By: [redacted]
Parkinson Larry R
Kelley Patrick W
[redacted]

Drafted By: [redacted] lml

Case ID #: 66-HQ-19490

Title: TECHNICALLY TRAINED AGENT (TTA) PROGRAM;
"USA PATRIOT ACT"

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-16-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

b6
b7C

Synopsis: This communication advises FBI Technically Trained Agents (TTAs) about relevant provisions in the USA Patriot Act.

Details: This communication is directed to FBI Technically Trained Agents (TTAs) and is intended to inform them about certain provisions in the recently-enacted antiterrorism USA Patriot Act ("Patriot Act" or "Act") (H.R. 3162), Public Law 107-56. The Patriot Act is a lengthy piece of legislation containing ten titles and numerous sections dealing with a broad array of antiterrorism provisions. Since many sections of the Act are not thought to be of interest to FBI TTAs, the information in this communication has been selected based on its perceived interest and value to TTAs. Full text of the Act can be obtained at [redacted] **www.access.gpo.gov/nara/index.html** (then go to "Catalogue of Public Law, 107th Congress, Public Law-107-056").

b5

Prior analyses regarding the Act have been provided and/or made available by the FBI Office of the General Counsel's National Security Law Unit **(NSLU)**(regarding FISA amendments and changes regarding the use of National Security Letters) and by the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), (regarding certain amendments to Title III; the Electronic Communications Privacy Act of 1986 (ECPA); Rule 41,

b5

Federal Rules of Criminal Procedure (Fed. R. Crim. P.); and to the substantive criminal law DOJ. [redacted] For those interested, review of the foregoing analyses is recommended since they afford greater elaboration upon many of the more important provisions in the Patriot Act.

The material set forth in the instant communication is offered only to present a brief synopsis of certain relevant provisions of the Act for TTAs. [redacted] b5

Notwithstanding the Act's organization of the material, for ease of discussion, the information set forth is grouped topically with reference to investigative, legal, and/or technical categories familiar to TTAs. In some cases, the material included draws substantially (and often verbatim) from analysis previously made available by the CCIPS, especially with regard to Sections 216 and 217 of the Act.

At the end of this EC, in topic area 9, in-depth guidance is provided to TTAs regarding the new "reporting" requirements under Section 216 with respect to a law enforcement agency's installation and use of a pen register/trap and trace using its own device on a packet-switched data network of a provider of electronic communication service to the public.

The topic areas drawn from in the Act and dealt with in this communication are:

1. Foreign Intelligence Surveillance Act (FISA)
Roving Authority
Greater Duration of FISA Electronic Surveillance
Change in FISA Pen Register/Trap Trace Showing
Greater Disclosure of FISA Electronic Surveillance Authorized
Change in Certification for Issuance of National Security Letters; Reduction in Approval Level
Computer Trespass Exception to FISA
Immunity for Compliance with a FISA Wiretap

2. Title III
Changes in Disclosure of Title III Interception Information
Obtaining Voice Mail/Stored Voice Communications Via a Search Warrant Rather than Title III
Harmonization of Procedures for Obtaining Communications, etc. with Respect to the Cable Act
Computer Trespass Exception to Title III

3. Stored Wire and Electronic Communications and Transactional Record Access
Information Available Pursuant to Subpoena
Nationwide Search Warrants for Stored Electronic Communications under 18 U.S.C. 2703
Emergency Disclosures by Communications Providers

4. Pen Register and Trap and Trace

Using Pen/Trap Orders to Acquire Communications Traffic Information on Computer Networks
Nationwide Effect of Pen/Trap Orders
Reports for Installation and Use of Law Enforcement Pen/Trap Devices on Computer Networks
No Imposition of Additional Technical Obligations on Service Providers or Others

5. Rule 41 Search Warrants
Single-Jurisdiction Search Warrants for Terrorism
Authority for Delaying Notice of the Execution of a Warrant

6. Civil Liability and Administrative Discipline for Certain Unauthorized Disclosures

7. Review of the Department of Justice

8. Congressional Support for Technology Centers; Task Forces; Role of Secret Service

Development and Support of Cybersecurity Forensic Capabilities
Expansion of the National Electronic Crime Force Initiative
Extension of Secret Service Jurisdiction

9. Section 216 Pen Register/Trap Trace Reporting Requirement

* * *

1. Foreign Intelligence Surveillance Act (FISA)

Roving Authority

b2
b7E

Section 206 of the Act amends FISA to afford "roving" electronic surveillance authority and service provider assistance under certain circumstances. The change is intended to be of assistance in coping with situations which arise when a FISA subject may be [redacted] The change brought about by this section indicates that a generic assistance order may be issued to address such situations. This approach is authorized when the FISA Court finds that the actions of the FISA subject may have the effect of thwarting the identification of such person/service provider. Although somewhat different, the concept here of roving interception technical "assistance" has some analogy to the assistance provision in Title III at 18 U.S.C. 2518(11)(b) and (12). This provision will sunset December 31, 2005.

Greater Duration of FISA Electronic Surveillance

Under Section 207 of the Act, the duration of a FISA electronic surveillance order is extended for non-U.S. persons who are agents of a foreign power (e.g., an officer or employee of foreign powers or a member of international terrorist organizations). Initial FISA electronic surveillance orders for such persons are now authorized for 120 days rather than the current 90 days, and extensions are now authorized for one year rather than the current 90 days. This provision will sunset December 31, 2005. ~~**This provision will sunset December 31, 2005.**~~

Change in FISA Pen Register/Trap Trace Showing

Section 214 of the Act simplifies the legal showing required to obtain a FISA pen register/trap trace order and expands the authority with respect to those subject to coverage. Now FISA pen register/trap trace orders can be obtained based upon a certification that the information likely to be obtained is foreign intelligence information not concerning a U.S. person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the 1st Amendment. A key aspect of the change is that the investigative effort need not be limited to a FISA subject per se or to the communication service used by such subject. Rather, under Section 214, the focus shifts to the likely relevance of the targeted communications to the types of investigations noted above. Thus, pen registers/trap traces with respect to persons in contact with a subject of such investigation can be authorized. This provision will sunset December 31, 2005.

Greater Disclosure of FISA Electronic Surveillance Authorized

Section 504 amends FISA, easing FISA electronic surveillance disclosure constraints, so as to permit those Federal officers conducting FISA electronic surveillance to acquire foreign intelligence information to consult with Federal law enforcement officers to coordinate efforts to investigate or protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage or international terrorism of a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. This change, along with others in the Act, removes barriers that heretofore had impeded appropriate sharing of such information with others with a clear need to know in the Government. Section 504, in concert with Section 218, also makes a change with respect to FISA's former requirement that foreign intelligence be "the" purpose (primary purpose) of the FISA surveillance. Now, the requirement is that foreign intelligence be a "significant purpose."

Change in Certification for Issuance of National Security Letters; Reduction in Approval Level

Section 505 of the Act changes the nature of the certification required for the issuance of National Security Letters (NSLs) under 18 U.S.C. 2709(b) and reduces the FBI approval level required for issuing such NSLs. NSLs are commonly used to obtain telephone toll and transactional records and subscriber information. Formerly, the issuance of NSLs was limited to investigations with respect to foreign counterintelligence. Now the nature of the certification required for issuing NSLs is that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the 1st Amendment. An authorized investigation means an investigation authorized under the Attorney General Guidelines for FCI investigations.

b2
b7E

Formerly, under 18 U.S.C. 2709, the Director of the FBI was authorized to delegate the issuance of NSLs to a level "not lower than Deputy Assistant Director" (meaning, effectively, to the Assistant Director/Deputy Assistant Director in the NSD and CTD at FBIHQ, and to the Assistant Director-in-Charge level in New York, Los Angeles, and WFO). The Act now permits the Director to also delegate such authority to specifically designated Special Agents-in-Charge in various FBI field offices.

Computer Trespass Exception to FISA

Section 1003 exempts from the requirement of obtaining a FISA court order the act of governmental interception of a computer trespasser's (e.g., "hacker's") unlawful communications transmitted to, through, or from a protected computer, when the interception is pursuant to valid computer owner consent, as now specified under 18 U.S.C. 2511(2)(i). This provision applies where a hacker or similar person accesses the "protected computer" (as that term is defined in18 U.S.C. 1030) of another in certain situations without authorization and thus without a reasonable expectation of privacy. The section mirrors a comparable amendment made to Title III in Section 217 of the Act. (*See* Section 217 below for greater explanation.)

Immunity for Compliance with a FISA Wiretap

Section 225 of the Act amends FISA to specify that no cause of action shall lie in any court against a provider of wire or electronic communication service, landlord, custodian, or other person that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under FISA. This provision mirrors a similar provision in Title III under 18 U.S.C. 2511(a)(ii), and is intended to remove any reticence that service providers and others might have in affording necessary FISA assistance to the Government owing to fears about potential civil causes of action being filed against them. This provision will sunset December 31, 2005.

2. Title III

Changes in Disclosure of Title III Interception Information

Section 203(b) of the Act amends Title III's disclosure provisions under 18 U.S.C.§ 2517. This section now permits an investigative or law enforcement officer or attorney for the Government who has lawfully intercepted communications or obtained evidence derived therefrom to disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in Section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information (as defined in subsection (19) of section 2510 of Title 18) to assist the official who receives that information in the performance of his official duties. Any Federal official receiving information pursuant to this provision may use the information only as necessary in the conduct of that person's official duties, subject to limitations on the unauthorized disclosure of such information. Under Section 203, the Attorney General is required to establish procedures for disclosure of such information that identifies a United States person, as defined in section 101 of FISA (50 U.S.C. 1801). Section 203(a) makes similar changes with respect to disclosure of grand jury information protected under Rule 6(e), Fed. R. Crim. P. This provision will sunset on December 31, 2005.

Obtaining Voice Mail/Stored Voice Communications via a Search Warrant Rather than Title III

Section 209 of the Act amends 18 U.S.C. §§ 2510 and 2703 to specify that stored wire communications are to be treated under the same rules applicable to stored electronic communications. Such stored wire communications can now be obtained from an electronic communications service provider using procedures set out in section 2703 (such as a search warrant), rather than arguably having to resort to a Title III court order. The Section 209 amendment does not apply to stored voice messages in the possession of an end-user person, such as those stored on an answering machine in a subject's home. Such non-service provider stored wire communications also remain outside the reach of Title III. This provision enacted in Section 209 will sunset on December 31, 2005.

Harmonization of Procedures for Obtaining Subscriber Communications, Records, and Information with Respect to the Cable Act

Section 211 amends the Communications Act of 1934 and the Cable Communications Policy Act of 1984 ("Cable Act")(47 U.S.C. § 551) to remove an apparent statutory conflict between provisions in the Cable Act and those set forth under Title III and the ECPA with respect to law enforcement obtaining a cable subscriber's communications, records, and information pertaining to such subscriber's telecommunications and/or Internet services. Prior to the Act's amendment, the Cable Act contained unworkable (and arguably unintended) provisions regarding law enforcement's obtaining a cable subscriber's communications, records, and information from the cable company as to telecommunications and/or Internet services offered by the cable company. Procedures under the Cable Act had most clearly been intended to protect subscriber privacy and information concerning cable video programming viewed by the subscriber. Section 211 makes it clear that, when a cable company offers services comparable to those offered by a telephone company or an ISP, the existing statutory provisions in Title III and the ECPA exclusively apply with respect to law enforcement's obtaining subscriber communications, records, and information in the cable company's control.

Computer Trespass Exception to Title III

Section 217 exempts from the requirement of obtaining a Title III court order the act of governmental interception of a computer trespasser's (e.g., "hacker's") communications transmitted to, through, or from a protected computer, when the interception is pursuant to valid computer owner consent, as now specified under 18 U.S.C. 2511(2)(i). This provision applies where a hacker or similar person accesses the "protected computer" (as that term is defined in 18 U.S.C. 1030) of another in certain situations without authorization and thus without a reasonable expectation of privacy. Because network service providers often lack the expertise, equipment, or financial resources required to monitor computer attacks themselves, in the past they commonly have had no effective way to exercise their rights to protect themselves from unauthorized attackers. Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims in taking natural and reasonable steps in their own defense that would be entirely legal in the physical world.

To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Before monitoring can occur, however, four requirements must be met under revised Section 2511(2). First, the owner or operator of the protected computer must

authorize the interception of the trespasser's communications on the protected computer. Second, the person acting under color of law who intercepts the communication must be lawfully engaged in an investigation applicable to such violation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, the person acting under color of law must have reasonable grounds to believe that the contents of the computer trespasser's communication to be intercepted will be relevant to the investigation. Fourth, the interception must be such that it does not acquire communications other than those transmitted to or from the computer trespasser. Thus, this section would only apply where the interception was effected such as to prevent the interception of communications of non-consenting users who are authorized to use the computer. The definition of computer trespasser explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). This provision will sunset December 31, 2005.

3. Stored Wire and Electronic Communications and Transactional Record Access

Information Available Pursuant to Subpoena

Section 210 of the Act amends title II of the ECPA, at 18 U.S.C. 2703(c), by updating and expanding the list and types of subscriber information and records law enforcement may obtain with a subpoena. Revised subsection 2703(c)(2) now includes "records of [Internet service] session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the service provider to the customer for a particular session, as well as the remote IP address from which a customer connects to the service provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier. In addition, the amendment specifies that a subpoena may be used to obtain the "means and source of payment" that a customer uses to pay for service with a service provider, "including any credit card or bank account number." Such information will prove particularly valuable in identifying the users of Internet services where a service provider does not verify its users' biographical information. The amendment adds to the subscriber information and records currently available pursuant to service of a subpoena (subscriber name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, length of service, and types of services utilized).

Nationwide Search Warrants for Stored Electronic Communications under 18 U.S.C. 2703

Section 220 of the Act amends 18 U.S.C. 2703 and 2711 so as to permit investigators to obtain and use search warrants authorized under section 2703(a) to acquire stored electronic communications (and, under Section 209 of the Act, stored wire communications) and records located outside of the district in which the court is located. This important change in the court's jurisdictional reach, giving search warrants authorized by the court under section 2703(a) national reach, puts search warrants on a comparable footing with the nationwide reach of federal grand jury subpoenas and court orders authorized under section 2703(d). This change enables courts with jurisdiction over investigations to authorize directly the search and seizure of stored wire and electronic communications and records located outside of the district in which the court is located; and it eliminates the necessity of having to obtain the additional involvement of agents, prosecutors, and judges in outside judicial districts, especially those in districts where major ISPs are located. This provision will sunset December 31, 2005.

Emergency Disclosures by Communications Providers

Section 212 of the Act amends 18 U.S.C. 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure does not create any affirmative obligation on the service provider to review customer communications in search of such imminent dangers.

Section 212 of the Act also amends the ECPA by allowing service providers to disclose information to protect *their* rights and property. It accomplishes this change by two related sets of amendments. First, amendments to 18 U.S.C. 2702 and 2703 simplify statutory treatment of voluntary disclosures by service providers by moving all such provisions to 2702. Thus, section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers only compulsory disclosures by service providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers *do* have the statutory authority to disclose non-content records to protect their rights and property. Prior to the Act, 2703 did not expressly permit a provider to voluntarily disclose *non-content* records (such as a subscriber's login records) to law enforcement for purposes of self-protection even though they could disclose the content of communications for this reason. These changes will sunset December 31, 2005.

4. Pen Register and Trap and Trace

Section 216 of the Act updates the pen register/trap trace ("pen/trap") statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to acquire non-content communications traffic information transmitted over the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install *their own* pen/trap device [redacted] on a packet-switched data network of a provider of electronic communication service to the public. b2 b7E

Using Pen/Trap Orders to Acquire Communications Traffic Information on Computer Networks

Section 216 of the Act amends 18 U.S.C. 3121, 3123, 3124, and 3127 to clarify that the pen/trap statute applies to a variety of communications technologies. References to the target "line," for example, are revised to encompass a "line or other facility." Such a facility might include, for example, a cellular telephone number/service; a specific cellular telephone identified by its electronic serial number (ESN); an Internet user account or e-mail address; or an Internet Protocol address, port number, or similar computer network address or range of addresses. In addition, because the law now clearly takes into account a wide variety of facilities, amendments to section 3123(b)(1)(C) allow applicants for pen/trap orders to submit a description of the communications traffic information to be acquired based upon any of these or other identifiers.

Moreover, the amendments clarify that pursuant to orders for the installation and use of pen/trap devices law enforcement may obtain any non-content information – [redacted] – utilized in the processing and transmitting of wire and electronic communications. [redacted] Pen/trap orders cannot, however, authorize the interception of the content of a communication, [redacted] b2 b7E

b5

example) non-content addressing ("to" and "from" or just "to") information over or through (what type of service): (Email/web etc.) ports, and whatever else the agency ~~would typically capture~~ [redacted] as a record of what had been done technically in the "settings" or "filters." In addition, when any changes to the settings, etc. are made, the record must include what the changes were (of course, along with the date/time and the name of the person(s) involved).

- As to subsection (iv), the record must identify:

The information which has been collected by the device. This information would **reflect** [redacted] the original (intelligible) evidentiary CD product that was obtained (e.g., the depiction of the "to" "from" information, "time," "duration," "port number,"any data acquired, etc.). [redacted] b5

Section 216 requires that "[t]o the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device." In short, if the law enforcement device can be configured electronically to automatically record the information noted above it must be done.

Once recorded, and maintained, the information must (shall) be provided (a) ex parte and (b) under seal to the court (c) within 30 days after the termination of the order (including any extension thereof). ~~The LAB believes that it~~ [redacted] should be the responsibility of the case agent, [redacted] to [redacted] submit the recorded information to [redacted] the AUSA handling the case. ~~who, in turn, will submit it to the magistrate judge who granted the original order.~~ [redacted] b5

A sample reporting format (below) is attached to aid in the reporting requirement as to subsections (i)-(iii). Obviously, as to subsection (iv), the information collected by the pen register or trap and trace device must be recorded (typically on a CD) and submitted to the court along with the foregoing information.

LEAD(s):

Set Lead 1:

ALL RECEIVING OFFICES

None. For information only.

CC: [redacted] b6 b7C

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 12/19/2001

To: Laboratory **Attn:** All ITB Section Chiefs
All ITB Unit Chiefs
All ITB Supervisory Special Agents
Technical Supervisors
Technical Advisors

All Field Offices

b2
b6
b7C

From: Laboratory
Investigative Technologies Branch
Contact: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-16-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

Approved By: Simons Allyson A [redacted]

b6
b7C

Drafted By: [redacted] lml

Case ID #: 66-HQ-19490

Title: TECHNICALLY TRAINED AGENT (TTA) PROGRAM;
"USA PATRIOT ACT"

Synopsis: This communication advises FBI Technically Trained Agents (TTAs) about relevant provisions in the USA Patriot Act.

Details: This communication is directed to FBI Technically Trained Agents (TTAs) and is intended to inform them about certain provisions in the recently-enacted antiterrorism USA Patriot Act ("Patriot Act" or "Act") (H.R. 3162), Public Law 107-56. The Patriot Act is a lengthy piece of legislation containing ten titles and numerous sections dealing with a broad array of antiterrorism provisions. Since many sections of the Act are not thought to be of interest to FBI TTAs, the information in this communication has been selected based on its perceived interest and value to TTAs. Full text of the Act can be obtained at **www.access.gpo.gov/nara/index.html.** Then go to "Catalogue of Public Law, 107th Congress, Public Law-107-056."

Prior analyses regarding the Act have been provided and/or made available by the FBI Office of the General Counsel's National Security Law Unit (regarding FISA amendments and changes regarding the use of National Security Letters) and by the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), (regarding certain amendments to Title III; the Electronic Communications Privacy Act of 1986 (ECPA); Rule 41, Federal Rules of Criminal Procedure (Fed. R. Crim. P.); and to the substantive criminal law). For those interested, review of the foregoing analyses is recommended since they afford greater elaboration upon many of the more important provisions in the Patriot Act.

The material set forth in the instant communication is offered only to present a brief synopsis of certain relevant provisions of the Act for TTAs. Notwithstanding the Act's organization of the material, for ease of discussion, the information set forth is grouped topically

with reference to investigative, legal, and/or technical categories familiar to TTAs. In some cases, the material included draws substantially (and often verbatim) from analysis previously made available by the CCIPS, especially with regard to Sections 216 and 217 of the Act.

At the end of this EC, in topic area 9, in-depth guidance is provided to TTAs regarding the new "reporting" requirements under Section 216 with respect to a law enforcement agency's installation and use of a pen register/trap and trace using its own device on a packet-switched data network of a provider of electronic communication service to the public.

The topic areas drawn from in the Act and dealt with in this communication are:

1. Foreign Intelligence Surveillance Act (FISA)
Roving Authority
Greater Duration of FISA Electronic Surveillance
Change in FISA Pen Register/Trap Trace Showing
Greater Disclosure of FISA Electronic Surveillance Authorized
Change in Certification for Issuance of National Security Letters; Reduction in Approval Level
Computer Trespass Exception to FISA
Immunity for Compliance with a FISA Wiretap

2. Title III
Changes in Disclosure of Title III Interception Information
Obtaining Voice Mail/Stored Voice Communications Via a Search Warrant Rather than Title III
Harmonization of Procedures for Obtaining Communications, etc. with Respect to the Cable Act
Computer Trespass Exception to Title III

3. Stored Wire and Electronic Communications and Transactional Record Access
Information Available Pursuant to Subpoena
Nationwide Search Warrants for Stored Electronic Communications under 18 U.S.C. 2703
Emergency Disclosures by Communications Providers

4. Pen Register and Trap and Trace

Using Pen/Trap Orders to Acquire Communications Traffic Information on Computer Networks
Nationwide Effect of Pen/Trap Orders
Reports for Installation and Use of Law Enforcement Pen/Trap Devices on Computer Networks
No Imposition of Additional Technical Obligations on Service Providers or Others

5. Rule 41 Search Warrants
Single-Jurisdiction Search Warrants for Terrorism
Authority for Delaying Notice of the Execution of a Warrant

6. Civil Liability and Administrative Discipline for Certain Unauthorized Disclosures

7. Review of the Department of Justice

8. Congressional Support for Technology Centers; Task Forces; Role of Secret Service

Development and Support of Cybersecurity Forensic Capabilities

Expansion of the National Electronic Crime Force Initiative
Extension of Secret Service Jurisdiction

9. Section 216 Pen Register/Trap Trace Reporting Requirement

* * *

b5

1. Foreign Intelligence Surveillance Act (FISA)

Roving Authority

Section 206 of the Act amends FISA to afford "roving" electronic surveillance authority and service provider assistance under certain circumstances. The change is intended to be of assistance in coping with situations which arise when a FISA subject may be [redacted] The change brought about by this section indicates that a generic assistance order may be issued to address such situations. This approach is authorized when the FISA Court finds that the actions of the FISA subject may have the effect of thwarting the identification of such person/service provider. Although somewhat different, the concept here of roving interception technical "assistance" has some analogy to the assistance provision in Title III at 18 U.S.C. 2518(11)(b) and (12). This provision will sunset December 31, 2005.

b2
b7E

Greater Duration of FISA Electronic Surveillance

Under Section 207 of the Act, the duration of a FISA electronic surveillance order s extended for non-U.S. persons who are agents of a foreign power (e.g., an officer or employee f foreign powers or a member of international terrorist organizations). Initial FISA electronic rveillance orders for such persons are now authorized for 120 days rather than the current 90 ys, and extensions are now authorized for one year rather than the current 90 days. This rovision will sunset December 31, 2005. This provision will sunset December 31, 2005.

Change in FISA Pen Register/Trap Trace Showing

Section 214 of the Act simplifies the legal showing required to obtain a FISA pen register/trap trace order and expands the authority with respect to those subject to coverage. Now FISA pen register/trap trace orders can be obtained based upon a certification that the information likely to be obtained is foreign intelligence information not concerning a U.S. person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a U.S. person is not conducted solely on the basis of activities protected by the 1st Amendment. A key aspect of the change is that the investigative effort need not be limited to a FISA subject per se or to the communication service used by such subject. Rather, under Section 214, the focus shifts to the likely relevance of the targeted communications to the types of investigations noted above. Thus, pen registers/trap traces with respect to persons in contact with a subject of such investigation can be authorized. This provision will sunset December 31, 2005.

term is defined in18 U.S.C. 1030) of another in certain situations without authorization and thus without a reasonable expectation of privacy. The section mirrors a comparable amendment made to Title III in Section 217 of the Act. (*See* Section 217 below for greater explanation.)

Immunity for Compliance with a FISA Wiretap

Section 225 of the Act amends FISA to specify that no cause of action shall lie in any court against a provider of wire or electronic communication service, landlord, custodian, or other person that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under FISA. This provision mirrors a similar provision in Title III under 18 U.S.C. 2511(a)(ii), and is intended to remove any reticence that service providers and others might have in affording necessary FISA assistance to the Government owing to fears about potential civil causes of action being filed against them. This provision will sunset December 31, 2005.

2. Title III

Changes in Disclosure of Title III Interception Information

Section 203(b) of the Act amends Title III's disclosure provisions under 18 U.S.C.§ 2517. This section now permits an investigative or law enforcement officer or attorney for the Government who has lawfully intercepted communications or obtained evidence derived therefrom to disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in Section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information (as defined in subsection (19) of section 2510 of Title 18) to assist the official who receives that information in the performance of his official duties. Any Federal official receiving information pursuant to this provision may use the information only as necessary in the conduct of that person's official duties, subject to limitations on the unauthorized disclosure of such information. Under Section 203, the Attorney General is required to establish procedures for disclosure of such information that identifies a United States person, as defined in section 101 of FISA (50 U.S.C. 1801). Section 203(a) makes similar changes with respect to disclosure of grand jury information protected under Rule 6(e), Fed. R. Crim. P. This provision will sunset on December 31, 2005.

Obtaining Voice Mail/Stored Voice Communications via a Search Warrant Rather than Title III

Section 209 of the Act amends 18 U.S.C. §§ 2510 and 2703 to specify that stored wire communications are to be treated under the same rules applicable to stored electronic communications. Such stored wire communications can now be obtained from an electronic communications service provider using procedures set out in section 2703 (such as a search warrant), rather than arguably having to resort to a Title III court order. The Section 209 amendment does not apply to stored voice messages in the possession of an end-user person, such as those stored on an answering machine in a subject's home. Such non-service provider stored wire communications also remain outside the reach of Title III. This provision enacted in Section 209 will sunset on December 31, 2005.

Harmonization of Procedures for Obtaining Subscriber Communications, Records, and Information with Respect to the Cable Act

Section 211 amends the Communications Act of 1934 and the Cable Communications Policy Act of 1984 ("Cable Act")(47 U.S.C. § 551) to remove an apparent statutory conflict between provisions in the Cable Act and those set forth under Title III and the ECPA with respect to law enforcement obtaining a cable subscriber's communications, records, and information pertaining to such subscriber's telecommunications and/or Internet services. Prior to the Act's amendment, the Cable Act contained unworkable (and arguably unintended) provisions regarding law enforcement's obtaining a cable subscriber's communications, records, and information from the cable company as to telecommunications and/or Internet services offered by the cable company. Procedures under the Cable Act had most clearly been intended to protect subscriber privacy and information concerning cable video programming viewed by the subscriber. Section 211 makes it clear that, when a cable company offers services comparable to those offered by a telephone company or an ISP, the existing statutory provisions in Title III and the ECPA exclusively apply with respect to law enforcement's obtaining subscriber communications, records, and information in the cable company's control.

Computer Trespass Exception to Title III

Section 217 exempts from the requirement of obtaining a Title III court order the act of governmental interception of a computer trespasser's (e.g., "hacker's") communications transmitted to, through, or from a protected computer, when the interception is pursuant to valid computer owner consent, as now specified under 18 U.S.C. 2511(2)(i). This provision applies where a hacker or similar person accesses the "protected computer" (as that term is defined in 18 U.S.C. 1030) of another in certain situations without authorization and thus without a reasonable expectation of privacy. Because network service providers often lack the expertise, equipment, or financial resources required to monitor computer attacks themselves, in the past they commonly have had no effective way to exercise their rights to protect themselves from unauthorized attackers. Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims in taking natural and reasonable steps in their own defense that would be entirely legal in the physical world.

To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Before monitoring can occur, however, four requirements must be met under revised Section 2511(2). First, the owner or operator of the protected computer must authorize the interception of the trespasser's communications on the protected computer. Second, the person acting under color of law who intercepts the communication must be lawfully engaged in an investigation applicable to such violation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, the person acting under color of law must have reasonable grounds to believe that the contents of the computer trespasser's communication to be intercepted will be relevant to the investigation. Fourth, the interception must be such that it does not acquire communications other than those transmitted to or from the computer trespasser. Thus, this section would only apply where the interception was effected such as to prevent the interception of communications of non-consenting users who are authorized to use the computer. The definition of computer trespasser explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). This provision will sunset December 31, 2005.

3. Stored Wire and Electronic Communications and Transactional Record Access

Information Available Pursuant to Subpoena

Section 210 of the Act amends title II of the ECPA, at 18 U.S.C. 2703(c), by updating and expanding the list and types of subscriber information and records law enforcement may obtain with a subpoena. Revised subsection 2703(c)(2) now includes "records of [Internet service] session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the service provider to the customer for a particular session, as well as the remote IP address from which a customer connects to the service provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier. In addition, the amendment specifies that a subpoena may be used to obtain the "means and source of payment" that a customer uses to pay for service with a service provider, "including any credit card or bank account number." Such information will prove particularly valuable in identifying the users of Internet services where a service provider does not verify its users' biographical information. The amendment adds to the subscriber information and records currently available pursuant to service of a subpoena (subscriber name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, length of service, and types of services utilized).

Nationwide Search Warrants for Stored Electronic Communications under 18 U.S.C. 2703

Section 220 of the Act amends 18 U.S.C. 2703 and 2711 so as to permit investigators to obtain and use search warrants authorized under section 2703(a) to acquire stored electronic communications (and, under Section 209 of the Act, stored wire communications) and records located outside of the district in which the court is located. This important change in the court's jurisdictional reach, giving search warrants authorized by the court under section 2703(a) national reach, puts search warrants on a comparable footing with the nationwide reach of federal grand jury subpoenas and court orders authorized under section 2703(d). This change enables courts with jurisdiction over investigations to authorize directly the search and seizure of stored wire and electronic communications and records located outside of the district in which the court is located; and it eliminates the necessity of having to obtain the additional involvement of agents, prosecutors, and judges in outside judicial districts, especially those in districts where major ISPs are located. This provision will sunset December 31, 2005.

Emergency Disclosures by Communications Providers

Section 212 of the Act amends 18 U.S.C. 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure does not create any affirmative obligation on the service provider to review customer communications in search of such imminent dangers.

Section 212 of the Act also amends the ECPA by allowing service providers to disclose information to protect *their* rights and property. It accomplishes this change by two related sets of amendments. First, amendments to 18 U.S.C. 2702 and 2703 simplify statutory treatment of voluntary disclosures by service providers by moving all such provisions to 2702. Thus, section 2702 now regulates all permissive disclosures (of content and non-content records

alike), while section 2703 covers only compulsory disclosures by service providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers *do* have the statutory authority to disclose non-content records to protect their rights and property. Prior to the Act, 2703 did not expressly permit a provider to voluntarily disclose *non-content* records (such as a subscriber's login records) to law enforcement for purposes of self-protection even though they could disclose the content of communications for this reason. These changes will sunset December 31, 2005.

4. Pen Register and Trap and Trace

Section 216 of the Act updates the pen register/trap trace ("pen/trap") statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to acquire non-content communications traffic information transmitted over the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install *their own* pen/trap device [redacted] on a packet-switched data network of a provider of electronic communication service to the public. b2 b7E

Using Pen/Trap Orders to Acquire Communications Traffic Information on Computer Networks

Section 216 of the Act amends 18 U.S.C. 3121, 3123, 3124, and 3127 to clarify that the pen/trap statute applies to a variety of communications technologies. References to the target "line," for example, are revised to encompass a "line or other facility." [redacted] b2 b7E In addition, because the law now clearly takes into account a wide variety of facilities, amendments to section 3123(b)(1)(C) allow applicants for pen/trap orders to submit a description of the communications traffic information to be acquired based upon any of these or other identifiers.

Moreover, the amendments clarify that pursuant to orders for the installation and use of pen/trap devices law enforcement may obtain any non-content information – [redacted] – utilized in the processing and transmitting of wire and electronic communications. [redacted] Pen/trap orders cannot, however, authorize the interception of the content of a communication, [redacted] Agents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context [redacted] or the Computer Crime and Intellectual Property Section in the computer context [redacted] b2 b7E

Further, because a pen/trap device [redacted] Section 216 makes two other related changes. First, in recognition of the fact that pen/trap functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen/trap device to be "attached or applied" to the target facility. Likewise, Section 216 revises the definitions of "pen register" and "trap and trace device" in section 3127 to include an intangible "process" (such as a software routine) which collects the same information as a physical device. b2 b7E

To: Laboratory From: Laboratory
Re: 66-HQ-19490, 12/19/2001

LEAD(s):

Set Lead 1:

ALL RECEIVING OFFICES

None. For information only.

CC: [redacted]

b6
b7C

♦♦

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 109
Page 1 ~ Referral/Direct
Page 2 ~ Referral/Direct
Page 3 ~ Referral/Direct
Page 5 ~ Referral/Direct
Page 6 ~ Referral/Direct
Page 7 ~ Referral/Direct
Page 8 ~ Referral/Direct
Page 9 ~ Referral/Direct
Page 10 ~ Referral/Direct
Page 11 ~ Referral/Direct
Page 12 ~ Referral/Direct
Page 13 ~ Referral/Direct
Page 14 ~ Referral/Direct
Page 15 ~ Referral/Direct
Page 16 ~ Referral/Direct
Page 17 ~ Referral/Direct
Page 19 ~ Referral/Direct
Page 20 ~ Referral/Direct
Page 21 ~ Referral/Direct
Page 22 ~ Referral/Direct
Page 24 ~ Referral/Direct
Page 25 ~ Referral/Direct
Page 26 ~ Referral/Direct
Page 27 ~ Referral/Direct
Page 29 ~ Referral/Direct
Page 30 ~ Referral/Direct
Page 31 ~ Referral/Direct
Page 32 ~ Referral/Direct
Page 33 ~ Referral/Direct
Page 34 ~ Referral/Direct
Page 35 ~ Referral/Direct
Page 36 ~ Referral/Direct
Page 37 ~ Referral/Direct
Page 38 ~ Referral/Direct
Page 39 ~ Referral/Direct
Page 40 ~ Referral/Direct
Page 41 ~ Referral/Direct
Page 42 ~ Referral/Direct
Page 43 ~ Referral/Direct
Page 44 ~ Referral/Direct
Page 45 ~ Referral/Direct
Page 46 ~ Referral/Direct
Page 47 ~ Referral/Direct
Page 48 ~ Referral/Direct

Page 49 ~ Referral/Direct
Page 50 ~ Referral/Direct
Page 51 ~ Referral/Direct
Page 107 ~ Referral/Direct
Page 108 ~ Referral/Direct
Page 109 ~ Referral/Direct
Page 110 ~ Referral/Direct
Page 111 ~ Referral/Direct
Page 112 ~ Referral/Direct
Page 113 ~ Referral/Direct
Page 114 ~ Referral/Direct
Page 115 ~ Referral/Direct
Page 116 ~ Referral/Direct
Page 117 ~ Referral/Direct
Page 118 ~ Referral/Direct
Page 119 ~ Referral/Direct
Page 120 ~ Referral/Direct
Page 121 ~ Referral/Direct
Page 122 ~ Referral/Direct
Page 123 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 128 ~ Referral/Direct
Page 129 ~ Referral/Direct
Page 130 ~ Referral/Direct
Page 131 ~ Referral/Direct
Page 132 ~ Referral/Direct
Page 133 ~ Referral/Direct
Page 134 ~ Referral/Direct
Page 135 ~ Referral/Direct
Page 136 ~ Referral/Direct
Page 137 ~ Referral/Direct
Page 138 ~ Referral/Direct
Page 139 ~ Referral/Direct
Page 140 ~ Referral/Direct
Page 141 ~ Referral/Direct
Page 142 ~ Referral/Direct
Page 143 ~ Referral/Direct
Page 144 ~ Referral/Direct
Page 145 ~ Referral/Direct
Page 146 ~ Referral/Direct
Page 147 ~ Referral/Direct
Page 148 ~ Referral/Direct
Page 149 ~ Referral/Direct
Page 150 ~ Referral/Direct
Page 151 ~ Referral/Direct
Page 152 ~ Referral/Direct
Page 153 ~ Referral/Direct
Page 154 ~ Referral/Direct

Page 155 ~ Referral/Direct
Page 156 ~ Referral/Direct
Page 157 ~ Referral/Direct
Page 158 ~ Referral/Direct
Page 159 ~ Referral/Direct
Page 160 ~ Referral/Direct
Page 161 ~ Referral/Direct
Page 162 ~ Referral/Direct
Page 163 ~ Referral/Direct
Page 164 ~ Referral/Direct
Page 165 ~ Referral/Direct
Page 166 ~ Referral/Direct
Page 167 ~ Referral/Direct
Page 168 ~ Referral/Direct

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, February 17, 2005 5:55 PM
To: [redacted] (OCA) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OCA) (FBI)
Subject: Comments on Feinstein Report

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179/DMH/JW/05-CV-0845

b6
b7C

[redacted] As per your request, attached are my comments on the Feinstein report drafted by DOJ. I put my comments right into the Word document. I ended up commenting on Sections 201, 203(d), and 209. I'll be out tomorrow, but will be here on Tuesday if you have any further questions.

[redacted]
ILU
x[redacted]

b2
b6
b7C

UNCLASSIFIED

Sunset Provisions

-

-

b5

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6

Sent: Thursday, March 17, 2005 1:41 PM b7C

To: [redacted] (OGC) (FBI)

Cc: [redacted] (OCA) (FBI); [redacted] (OGC) (FBI)

Subject: FISA - change in primary purpose standard - sunset provision - Homeland Security Act

UNCLASSIFIED
NON-RECORD

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179/DMH/JW/05-CV-0845

[redacted]

b2
b5

I've been working with OCA [redacted] et al) to support the efforts on the Hill to seek renewal of the Patriot Act sunset provisions. [redacted] b6 b7C

[redacted] b5

[redacted] b5

[redacted] b5

Please feel free to call me so we can discuss this further. I look forward to your response.

Thanks.

[redacted]
ILU
[redacted]

b2
b6
b7C

UNCLASSIFIED

[redacted] (OGC) (FBI) b6 b7C

From: [redacted] (OGC) (FBI)
Sent: Thursday, March 24, 2005 1:30 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OCA) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: FISA - change in primary purpose standard - sunset provision - Homeland Security Act

UNCLASSIFIED
NON-RECORD

[redacted] b2 b5 b6 b7C

Thanks for clearing this up for me.

[redacted] b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179/DMH/JW/05-CV-0845

-----Original Message-----
From: [redacted] (OGC) (FBI) b6 b7C
Sent: Friday, March 18, 2005 8:40 AM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OCA) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: FISA - change in primary purpose standard - sunset provision - Homeland Security Act

UNCLASSIFIED
NON-RECORD

b5 b6 b7C

Thank you [redacted]

I am assigning this to [redacted] to research and answer your questions. b6 b7C

[redacted]
National Security Law Policy and Training Unit
FBI HQ Room 7975
[redacted] b2 b6 b7C
Unclassified Fax: [redacted]
Secure Fax: [redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 17, 2005 1:41 PM

b6 b7C

b6
b7C

To: (OGC) (FBI)
Cc: OCA) (FBI); (OGC) (FBI)
Subject: FISA - change in primary purpose standard - sunset provision - Homeland Security Act

UNCLASSIFIED
NON-RECORD

b6
b7C

-

I've been working with OCA (et al) to support the efforts on the Hill to seek renewal of the Patriot Act sunset provisions.

b2
b5
b6
b7C

b5

b5

b5

Please feel free to call me so we can discuss this further. I look forward to your response.

Thanks.

ILU
x

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI)

From: [redacted](OGC) (FBI)
Sent: Thursday, March 24, 2005 6:34 PM
To: [redacted](OCA) (FBI) b6
Subject: Comments on Feinstein Sunset Report b7C

UNCLASSIFIED
NON-RECORD

b6
[redacted] - Attached is the draft report including my comments. I had more time to review the document than the b7C
previous time, so I have a few more comments. I put the comments right into the document. Should you have any questions, please feel free to contact me. I will be out of the office until 4/5.

Thanks.

b2
[redacted] b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179/DMH/JW/05-CV-0845

-----Original Message-----
From: [redacted](OCA) (FBI) b6
Sent: Tuesday, March 15, 2005 6:34 PM b7C
To: [redacted](OGC) (FBI)
Cc: [redacted](OGC) (FBI)
Subject: RE: Delayed Notice Search Warrants AND SUNSET GENERALLY

UNCLASSIFIED
NON-RECORD

b6
[redacted] - whew - it's been a busy day. The best DOJ poc for guidance on Patriot Act issues is Rachel b7C
Brand or Matthew Berry or Beth LNU of DOJ OLP. Beth LNU just came on board this week and is in the process of getting up to speed on Patriot Act issues.

Re §213 specifically, DOJ is in the process of finalizing a letter re this provision. I think a draft was circulated over the weekend, but since the Internet Cafe has been up and down, I didn't receive it. When b6
it's done, I think it will be the DOJ official position / guidance on the provision. I'll circulate a copy to you b7C
and [redacted] as soon as I see it in draft or final.

Re sunsets generally, I've attached the final draft report on Sunset provisions. This is the same document that you reviewed last month - we just get a final stab. If you have time and can take a look, I'd appreciate it. I'll also route to Julie Thomas in NSLB.

Thanks,

[redacted] b2
Office of Congressional Affairs b6
[redacted] b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Tuesday, March 15, 2005 1:11 PM
To: [redacted](OCA) (FBI) b6
b7C

b6
b7C

Cc: [redacted]
Subject: Delayed Notice Search Warrants.

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] - When DOJ issued guidance initially after the Patriot Act was passed, they noted that they would issue additional guidance on this provision. I checked with the DOJ Crim Div. about a year later to locate this guidance and to no avail. In all your various discussions with DOJ on this provision, have you come across any guidance? Do you have a POC at DOJ on this provision? (Section 213)

We don't have a pressing issue, just want to ensure that we have complete copies of all guidance issued on this provision.

Thanks.

b2
b6
b7C

[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI)

From: [redacted]OCA) (FBI)
Sent: Monday, April 04, 2005 9:13 AM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: Patriot Act Sunset Provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

fyi - attached is a report that DOJ sent to the Hill on Friday re Patriot Act sunset provisions.

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

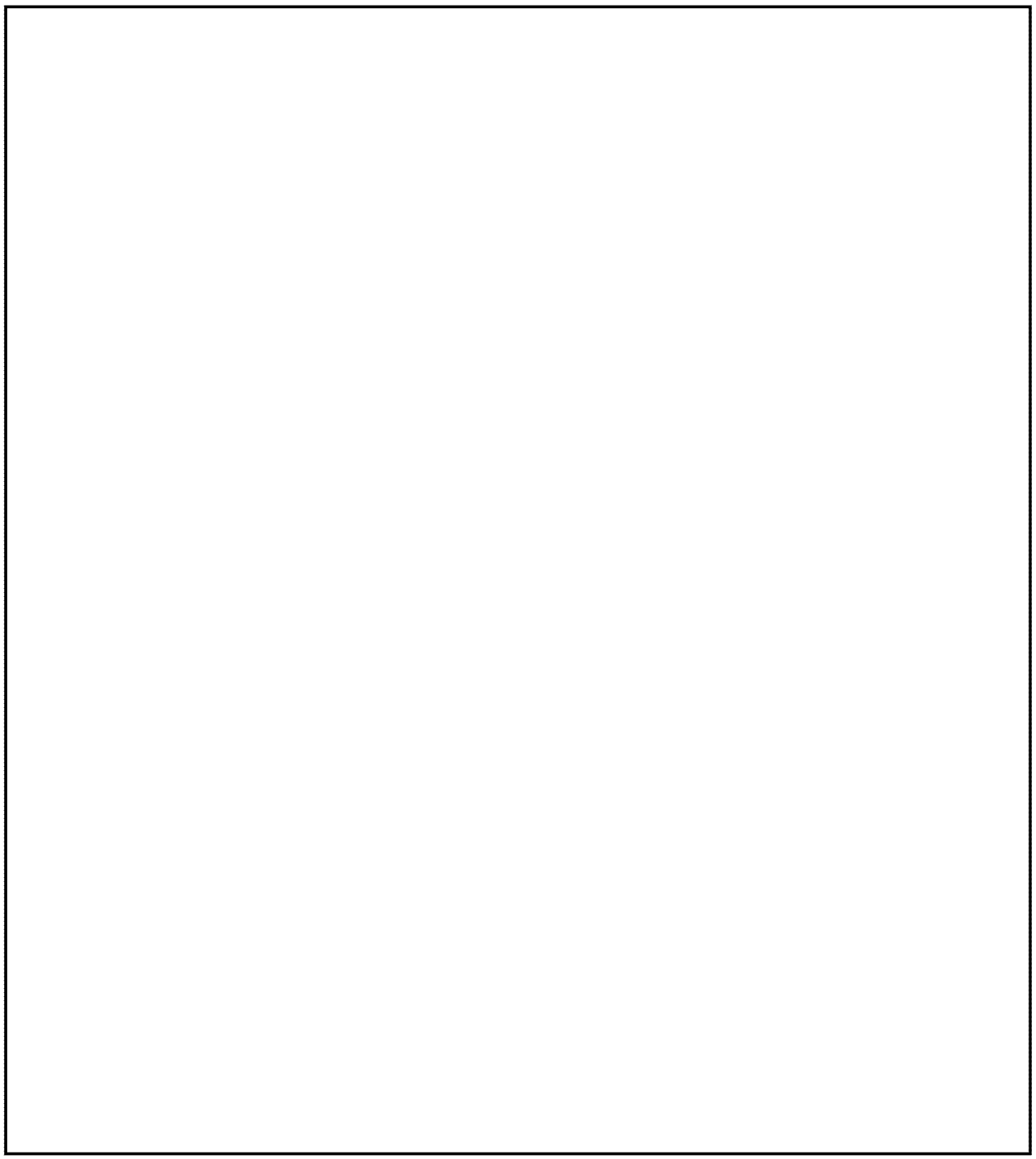
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179/DMH/JW/05-CV-0845

UNCLASSIFIED

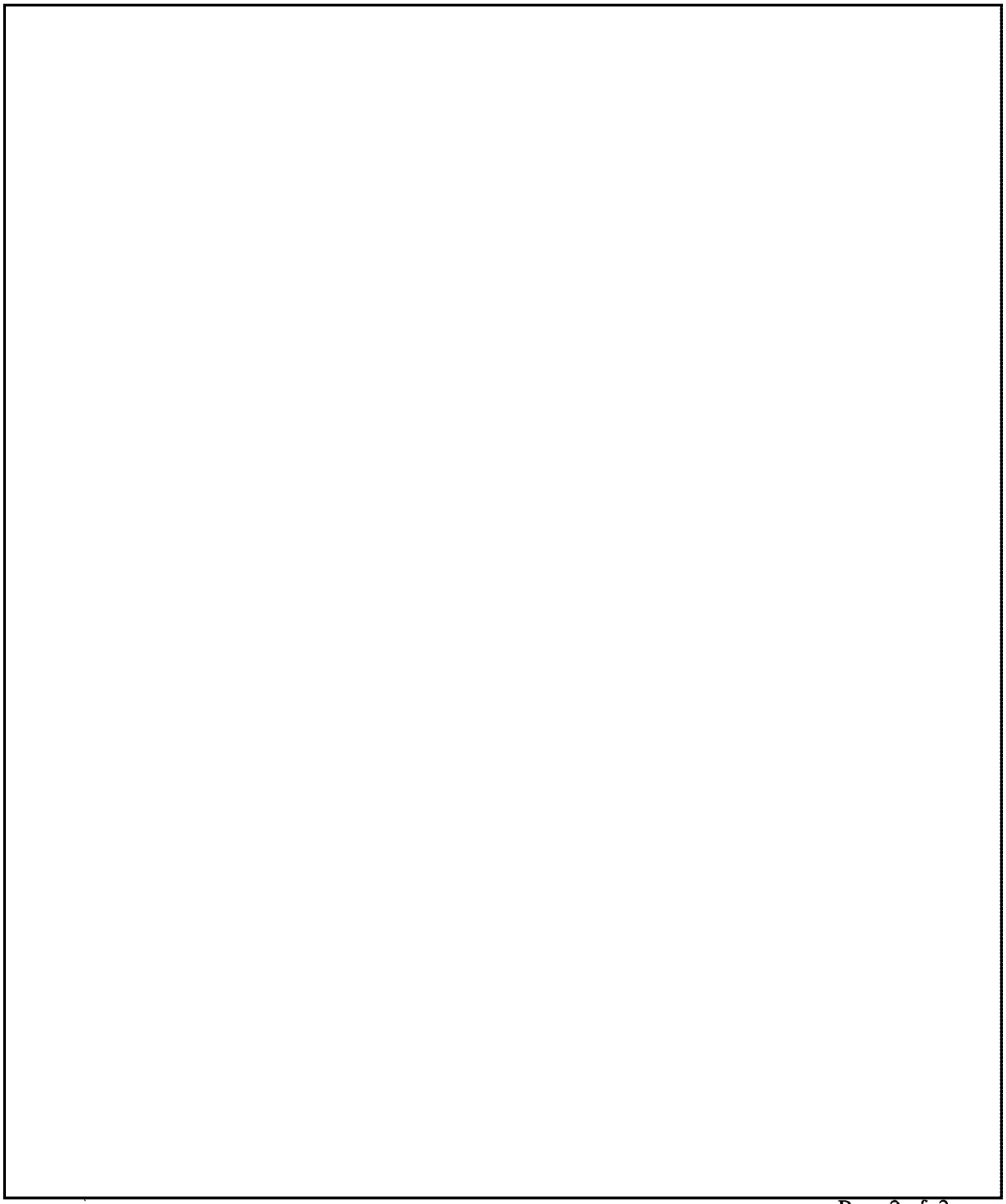
DRAFT

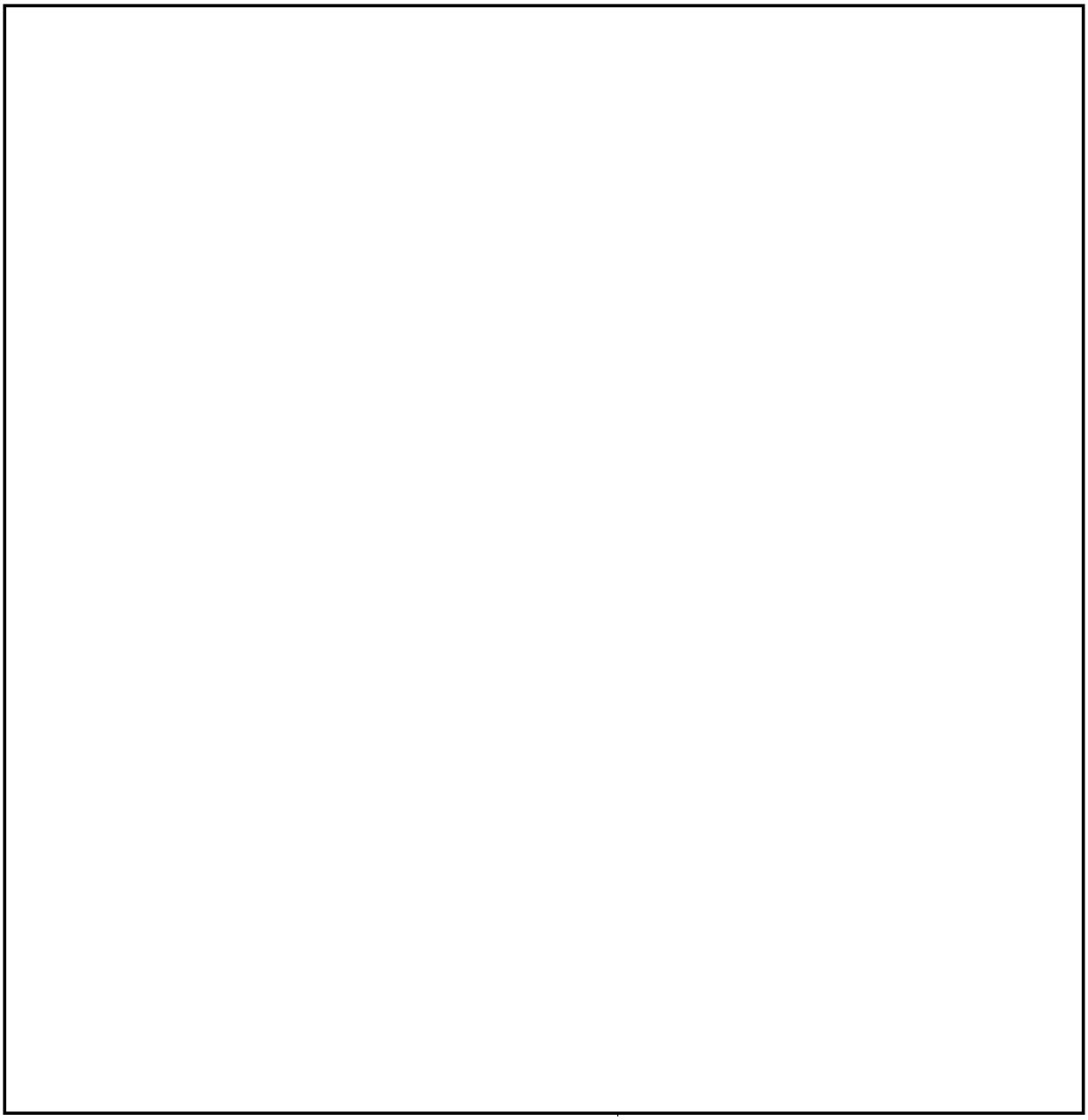
USA Patriot Act
Sunset Provisions

b5



b5





b2
b5
b7E

Section	Includes Non-terrorism Investigations[1]	Only Terrorism Investigations
203(a)	Information Sharing (grand jury)	
203(b)	Information Sharing (Title III)	
203(d)	Information Sharing (intelligence info obtained in the course of a criminal invesgation)	
206	Roving FISA Authority	
207	Extended duration of FISA authority	
209	Voice mail - can be obtained with a search warrant	
210	Expanded subscriber information that can be obtained with a subpoena	
212	Voluntary disclosures by Internet Service Providers for emergencies	
213	Delayed notice for search warrants (sneek and peak warrants)	
214	FISA - change to pen/trap standard	
215	FISA - Business Records	
216	Nationwide effect of pen/trap orders	
217	Computer tresspasser exception to the wiretap statute	
218	FISA - changes "primary purpose" standard to "significant purpose"	
219		Nationwide search warrants
220	Nationwide search warrants for e-mail	
225	Grants immunity from civil liability for persons providing information in response to FISA order.	

375	Increased penalities for counterfeiting foreign currency	
376		Expanded money laundering predicates to include providing material support to foreign terrorists organizations.
377	Creates extra-territorial jurisdiction for fraud related to access devices (18 U.S.C. § 1029 - often used in computer related crimes involving stolen credit card numbers.)	
411		Expands terrorism related definitions for immigration statutes.Grants to state/locals to enhance ability to respond to terrorist acts. [redacted] b5
412	Requires AG to detain aliens that he certifies as threats to national security.	
413	Provides ability to share visa-records information with foreign governments	
416	Requires AG to expand foreign student visa monitoring program.	
503	Expands predicates for collection of DNA samples.	
504	Authorized sharing of FISA information with federal law enforcement officers	
505	Changed standards for obtaining NSLs	
507		Access to educational records

Section	Includes Criminal and Terrorism Investigations	Terrorism and CI Investigations	Only Terrorism Investigations
203(a)		Information Sharing (Grand Jury)	
203(b)		Information Sharing (Title III)	
203(d)		Information Sharing (intelligence info obtained in the course of a criminal investigation)	
206		Roving FISA Authority	
207		Extended duration of FISA authority - also expanded FISC	
209	Voice mail - can be obtained with a search warrant		
210	Expanded subscriber information that can be obtained with a subpoena		
212	Voluntary disclosures by Internet Service Providers for emergencies		
213	Delayed notice for search warrants (sneak and peak warrants)		
214		FISA - change to pen/trap standard	
215		FISA - changed standard for business records authority	
216	Nationwide effect of pen/trap orders		
217	Computer trespasser		

	exception to the wiretap statute		
218		FISA - changes "primary purpose" standard to "significant purpose"	
219			Nationwide search warrants
220	Nationwide search warrants for e-mail		
223	OPR inquiry for improper disclosure of information pursuant to TIII, ECPA, pen/trap and trace, NSLs	Established civil liability for unauthorized disclosure of FISA information	
225		Grants immunity from civil liability for persons providing information in response to FISA order.	
Money Laundering			
314	Cooperative efforts between government and financial institutions to deter money laundering (aimed at, but not limited to, terrorist financing)		
315	Expanded money laundering predicates		
317 & 318	Long-arm jurisdiction over foreign money launderers		

Section	Includes Non-terrorism Investigations[1]	Only Terrorism Investigations
203(a)	Information Sharing (grand jury)	
203(b)	Information Sharing (Title III)	
203(d)	Information Sharing (intelligence info obtained in the course of a criminal invesgation)	
205		Employment of Translators
206	Roving FISA Authority	
207	Extended duration of FISA authority	
209	Voice mail - can be obtained with a search warrant	
210	Expanded subscriber information that can be obtained with a subpoena	
211	Clarified that the cable providers that also provide Internet service are governed by the same laws regarding disclosure of records to the government.	
212	Voluntary disclosures by Internet Service Providers for emergencies	
213	Delayed notice for search warrants (sneek and peak warrants)	
214	FISA - change to pen/trap standard	
215	FISA - Business Records	
216	Nationwide effect of pen/trap orders	
217	Computer tresspasser exception to the wiretap statute	
218	FISA - changes "primary purpose" standard to "significant purpose"	
219		Nationwide search warrants
220	Nationwide search warrants for e-mail	

~~SECRET~~

b1 ,b2, b6, b7C, b7D, b7E

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

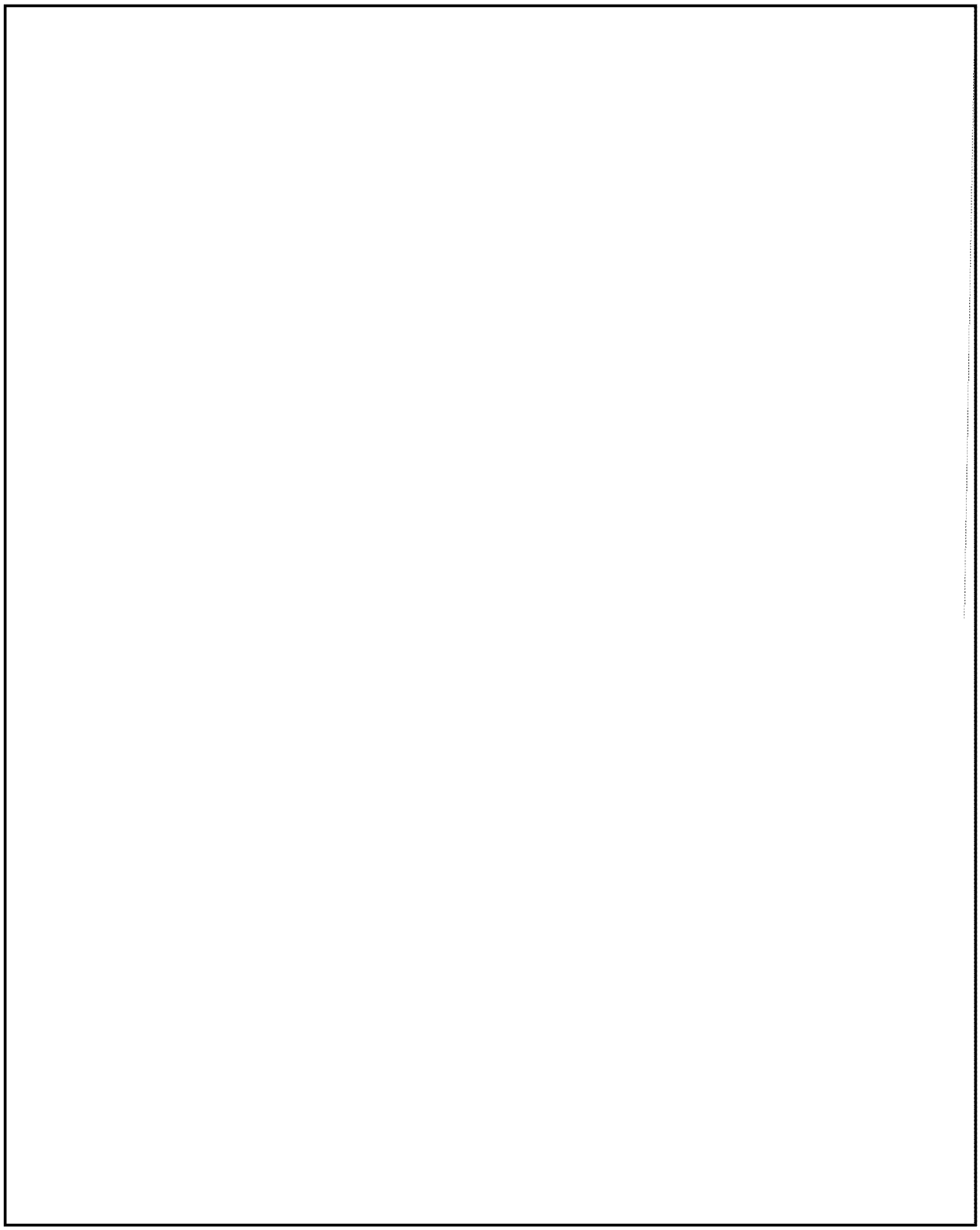
April 19, 2004

DATE: 08-25-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C) (D)
DECLASSIFY ON: 08-25-2030

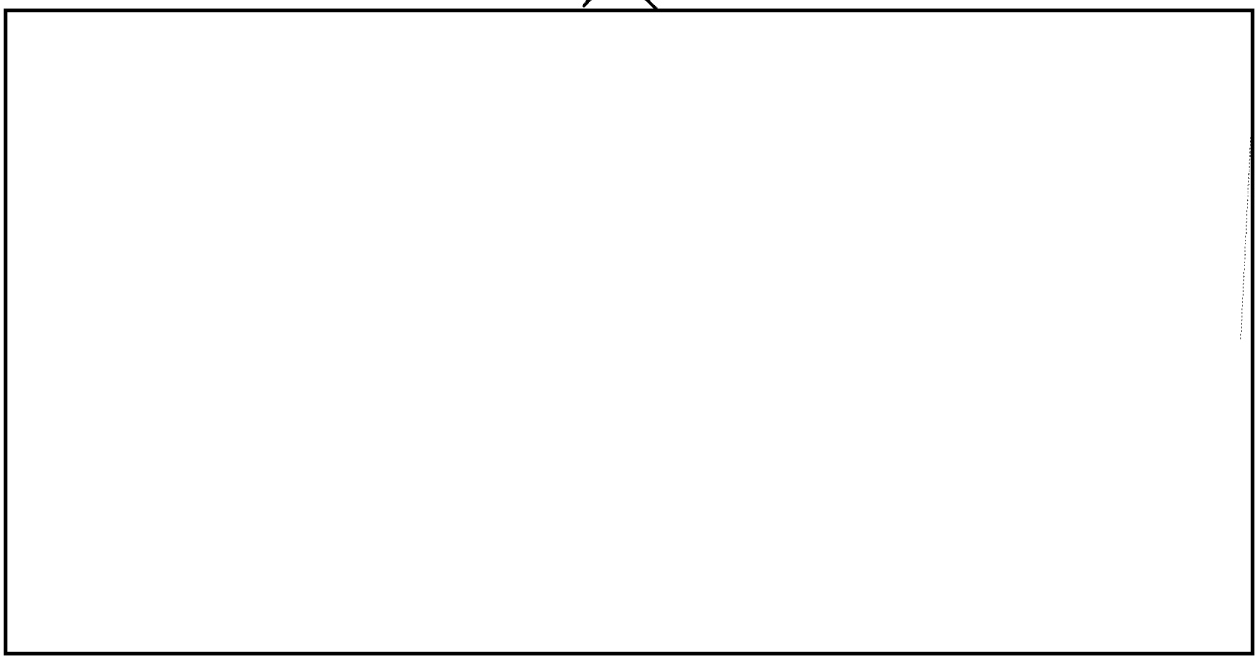
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

~~SECRET~~



(S)



(S)

b1
b2
b6
b7C

(Rev. 01-31-2003)

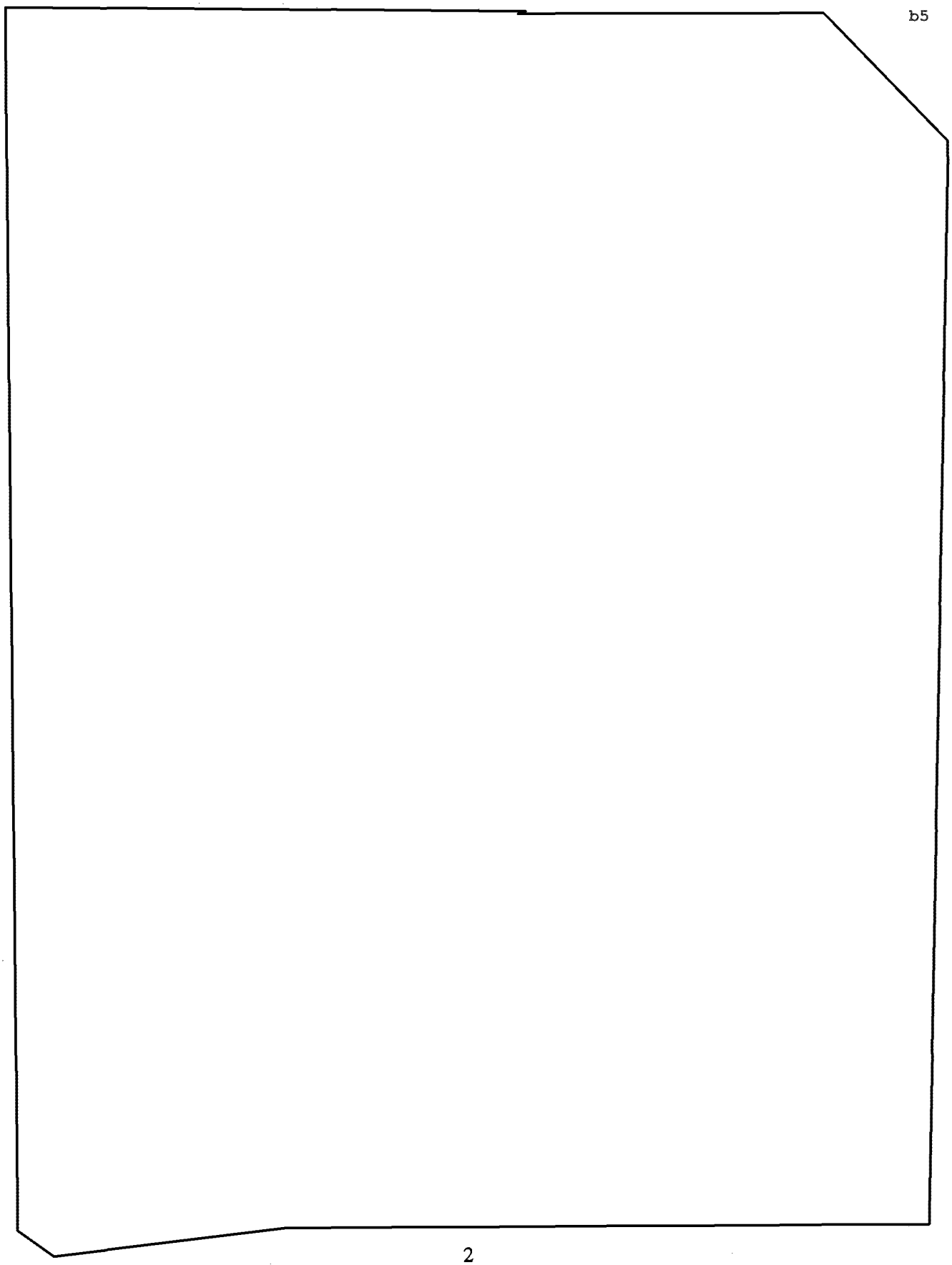
FEDERAL BUREAU OF INVESTIGATION

DRAFT

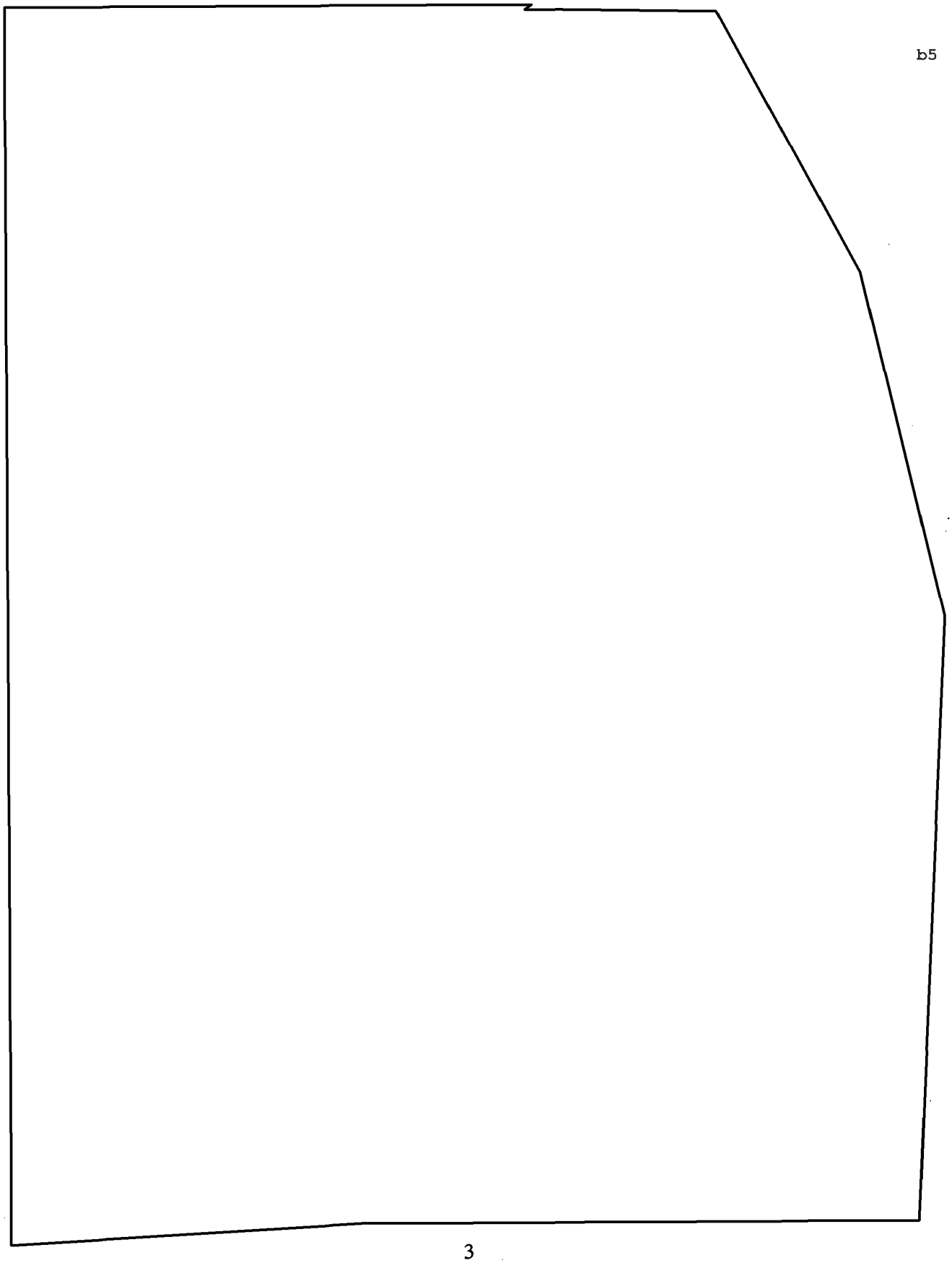
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179/DMH/JW/05-CV-0845

b2
b5
b6
b7C

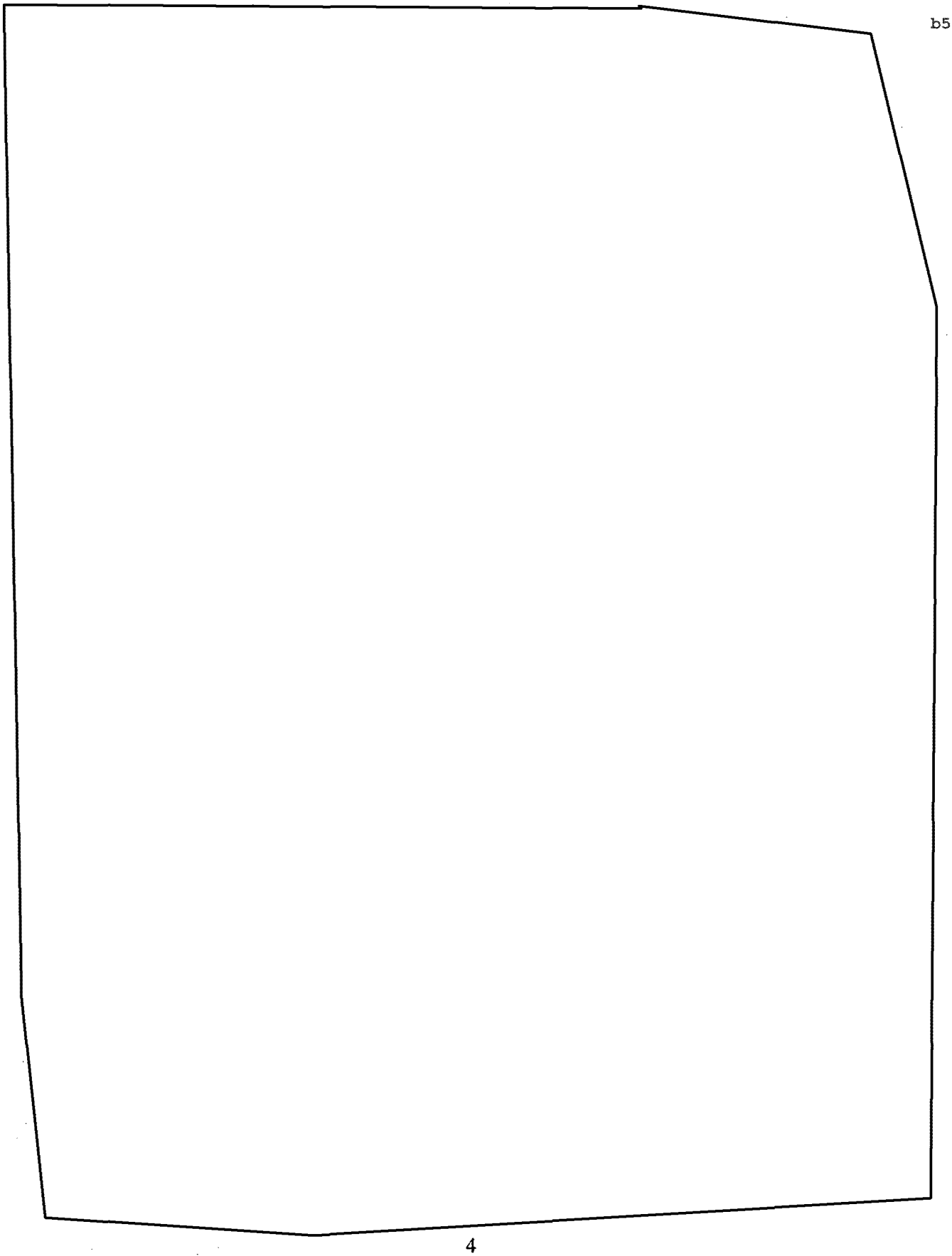
b5



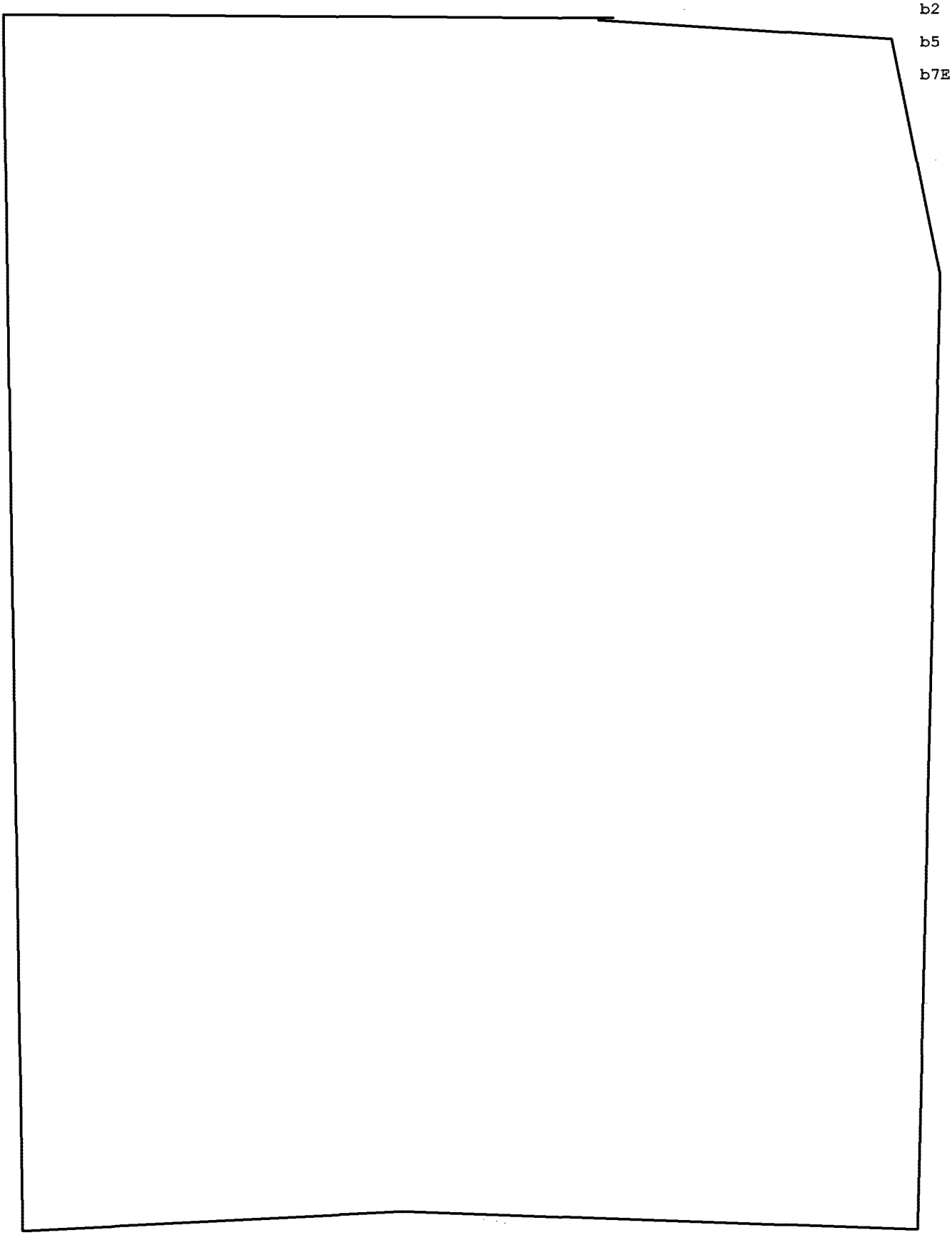
b5



b5



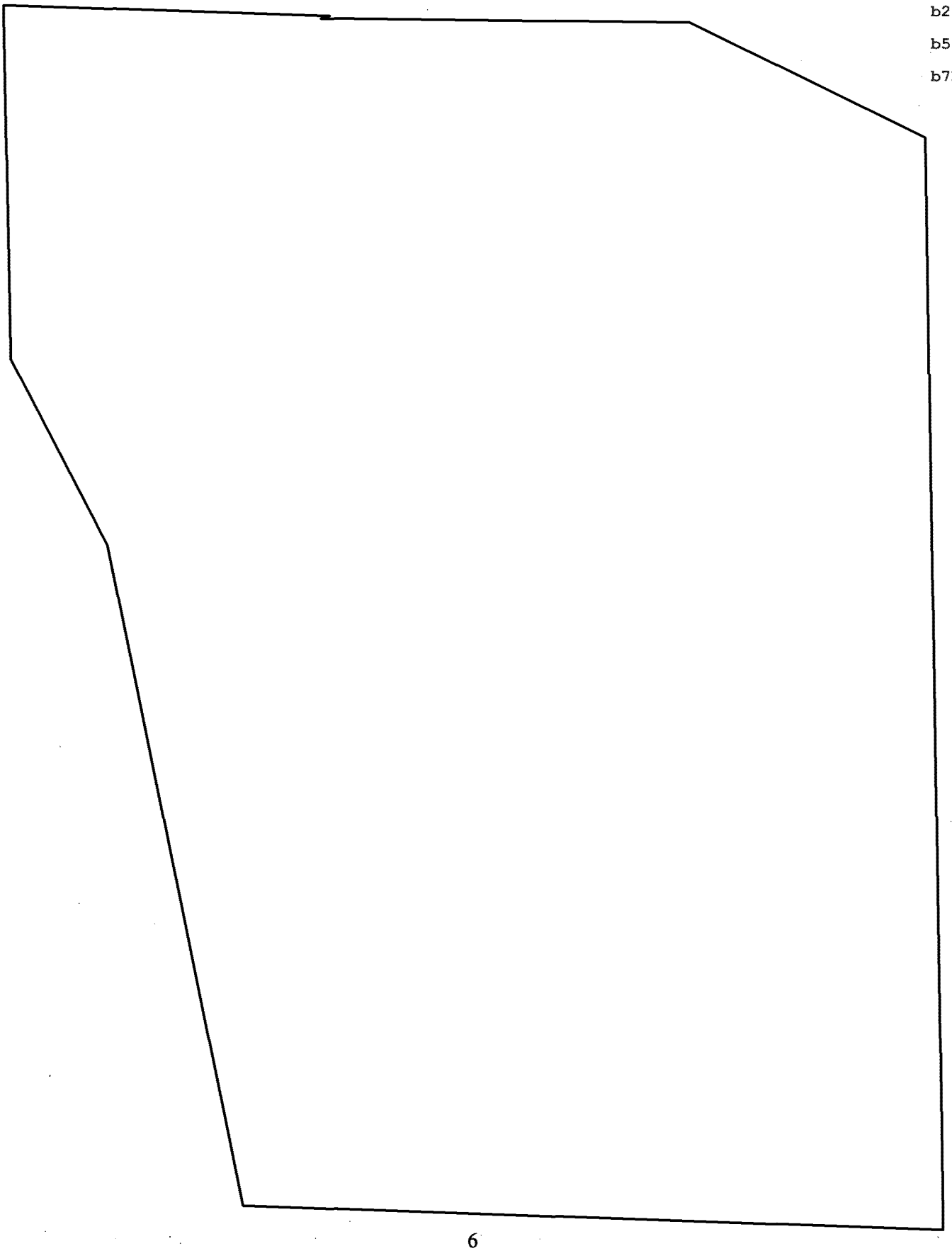
b2
b5
b7E

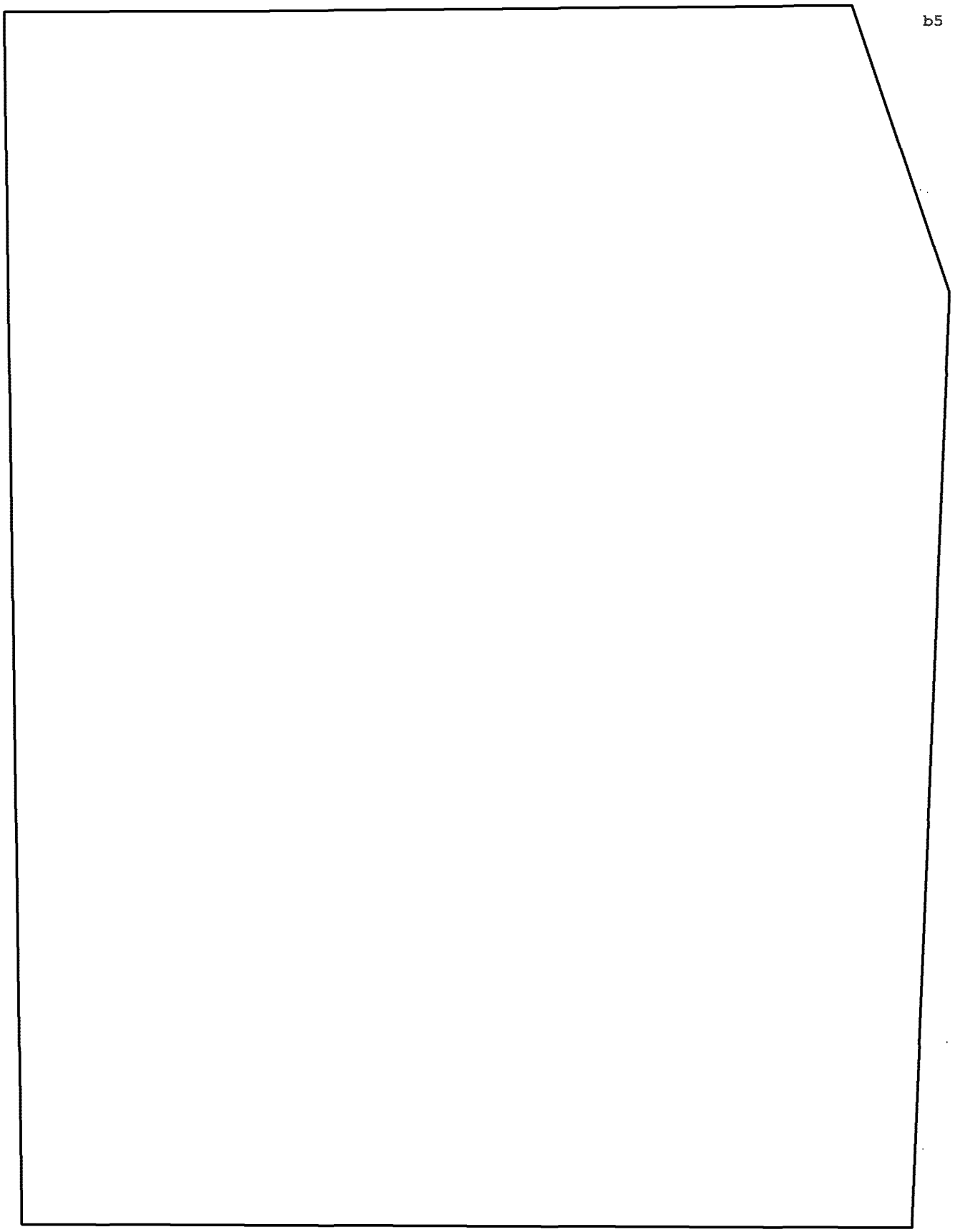


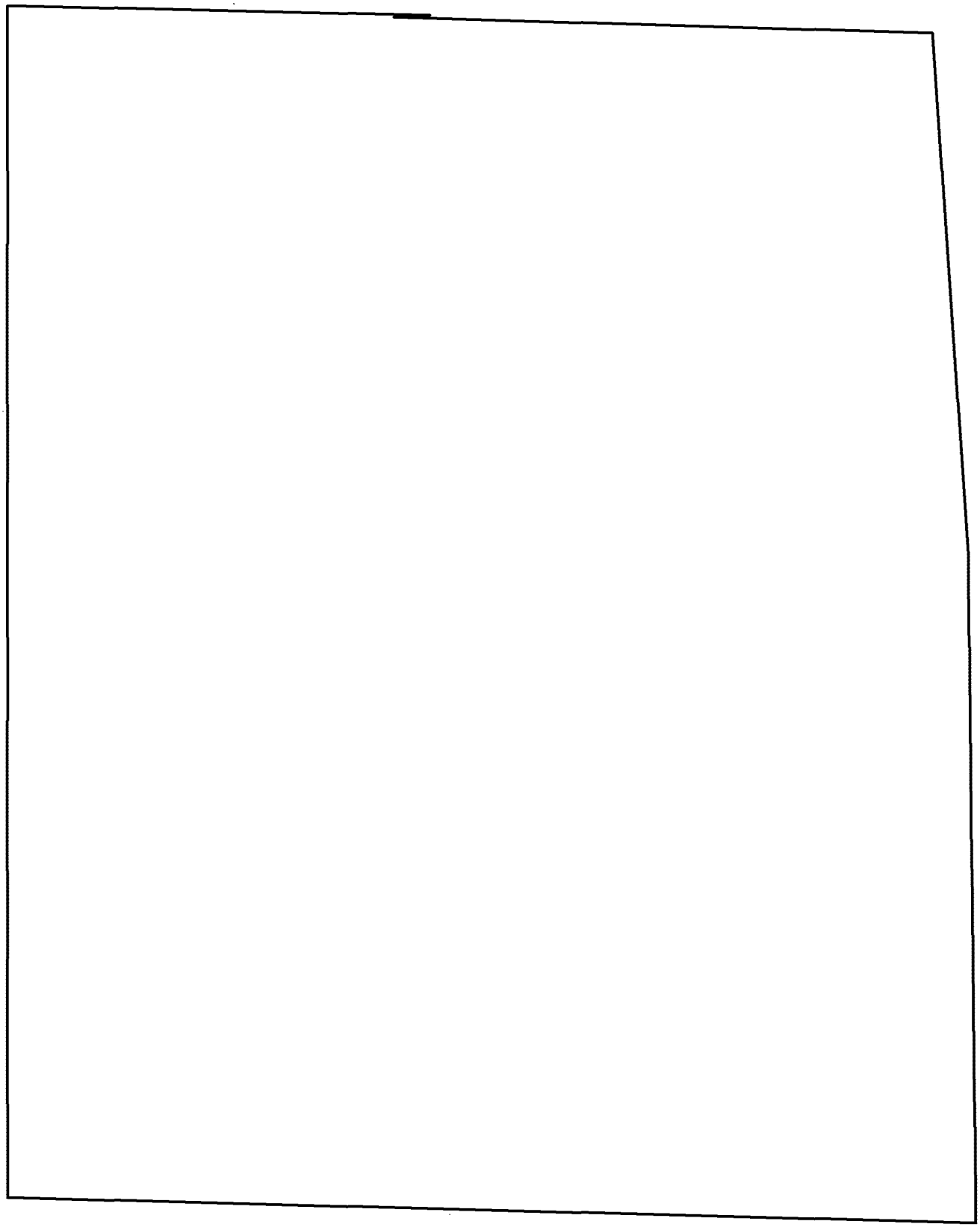
b2

b5

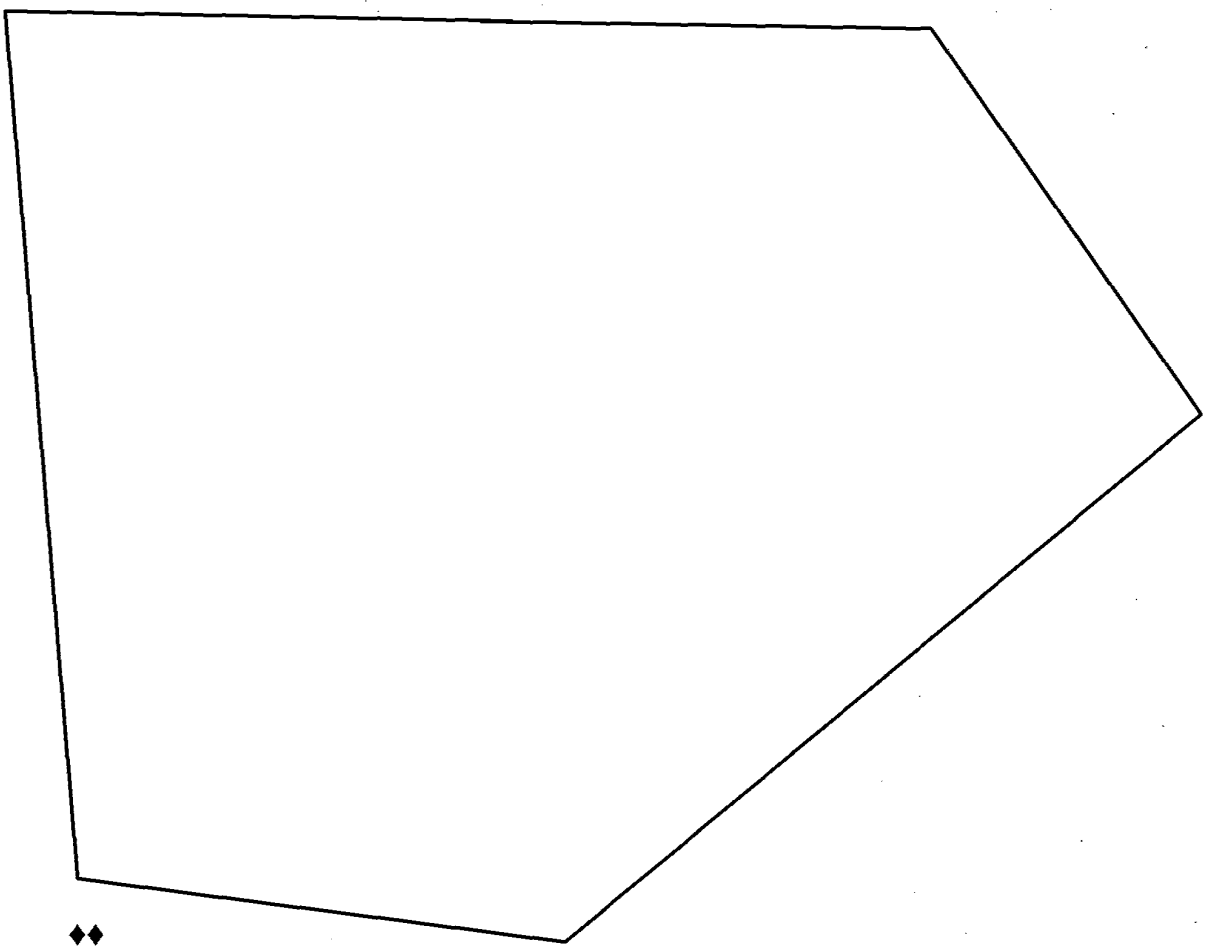
b7E




b5



b2
b5
b6
b7C
b7E



b5

b6

b7C

♦♦

(Rev. 01-31-2003)

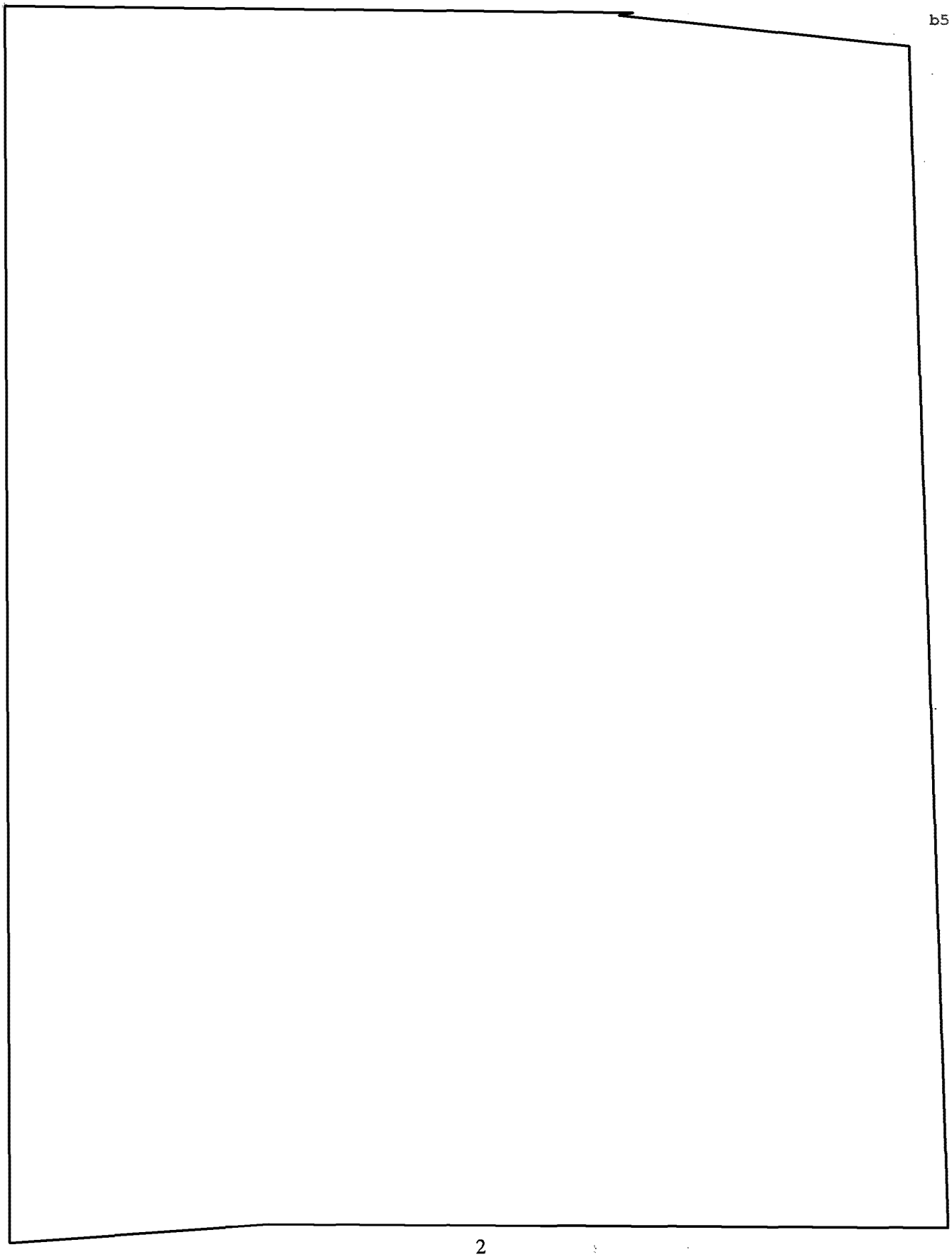
b5
b6
b7C

FEDERAL BUREAU OF INVESTIGATION

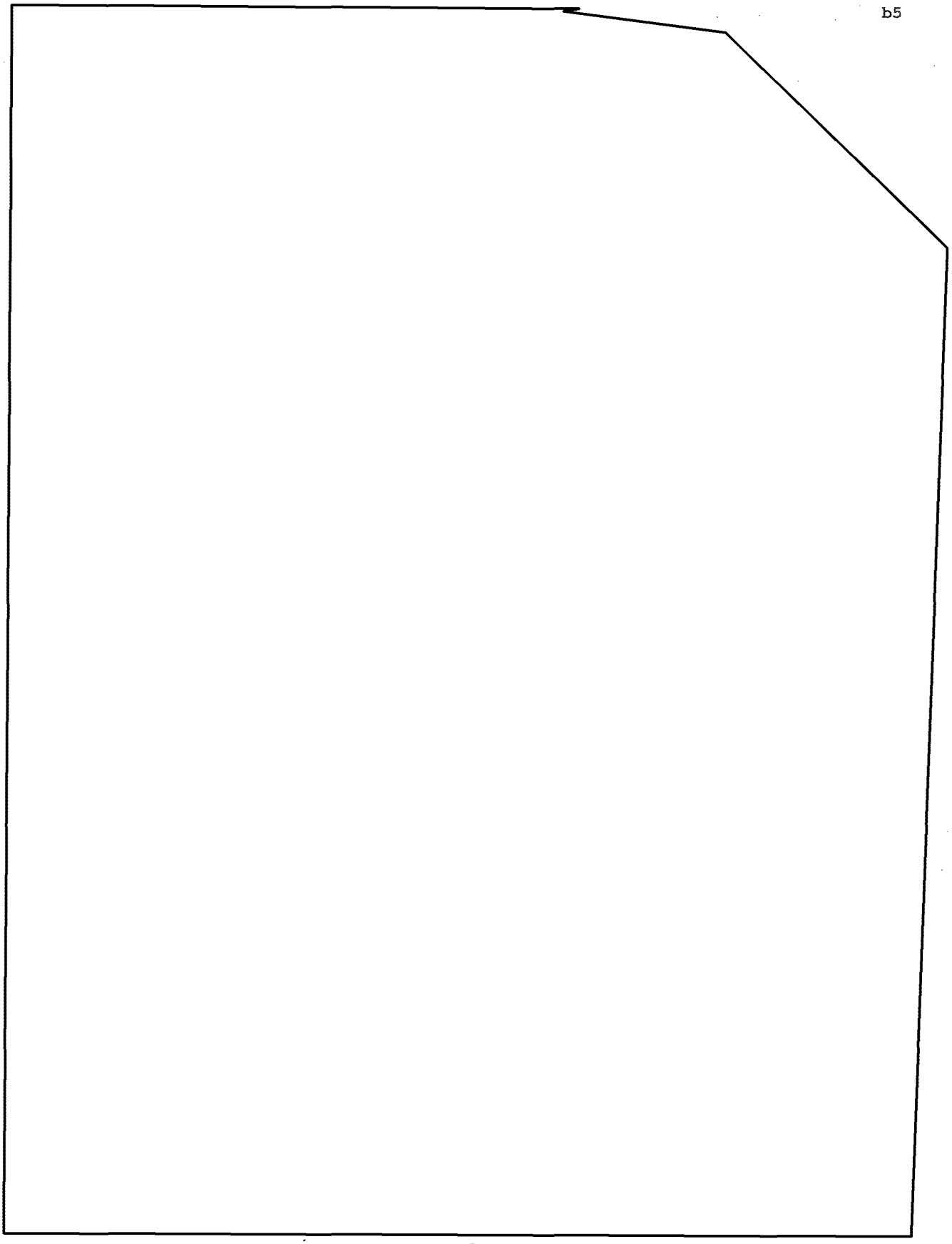
DRAFT

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179/DMH/JW/05-CV-0845

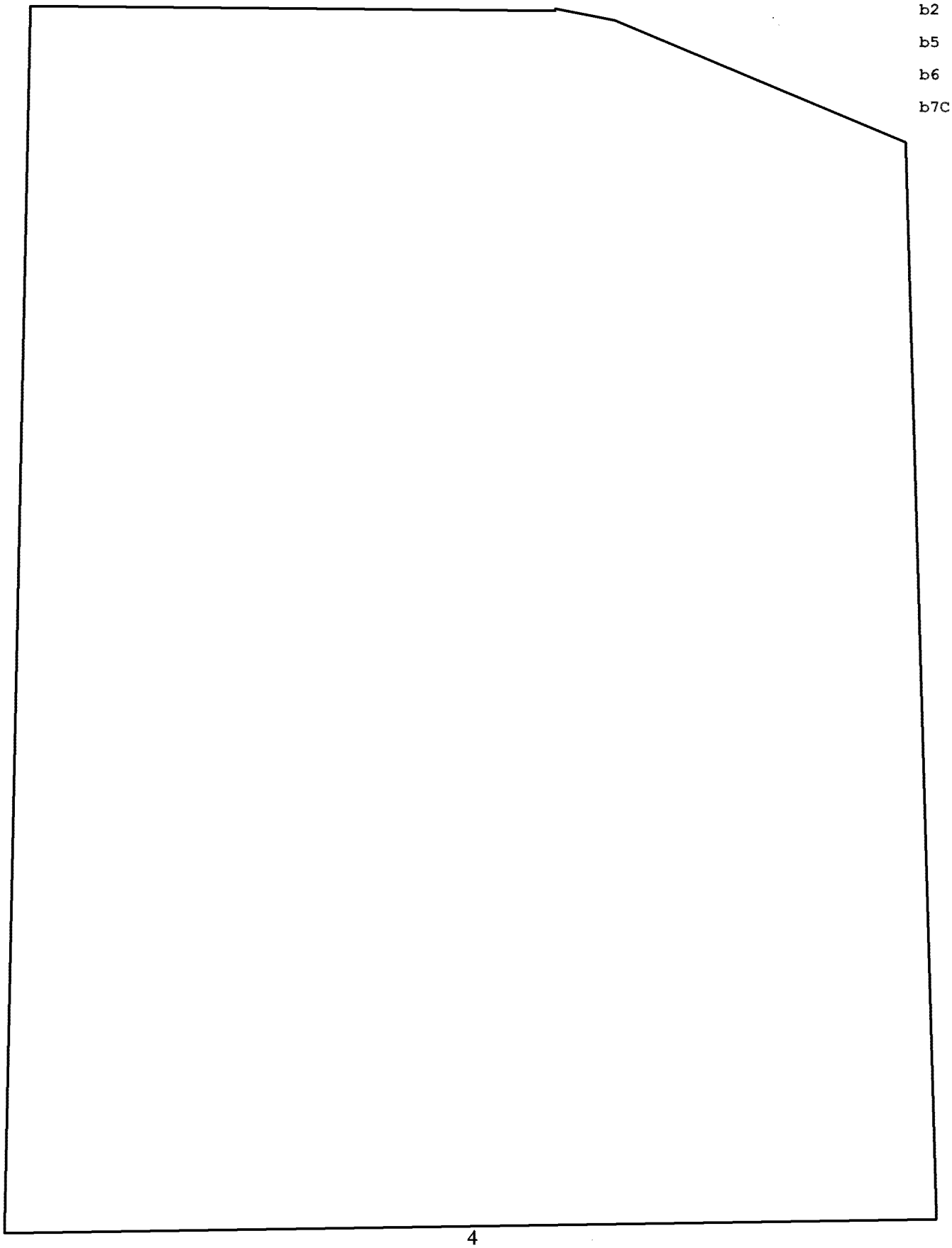
b5



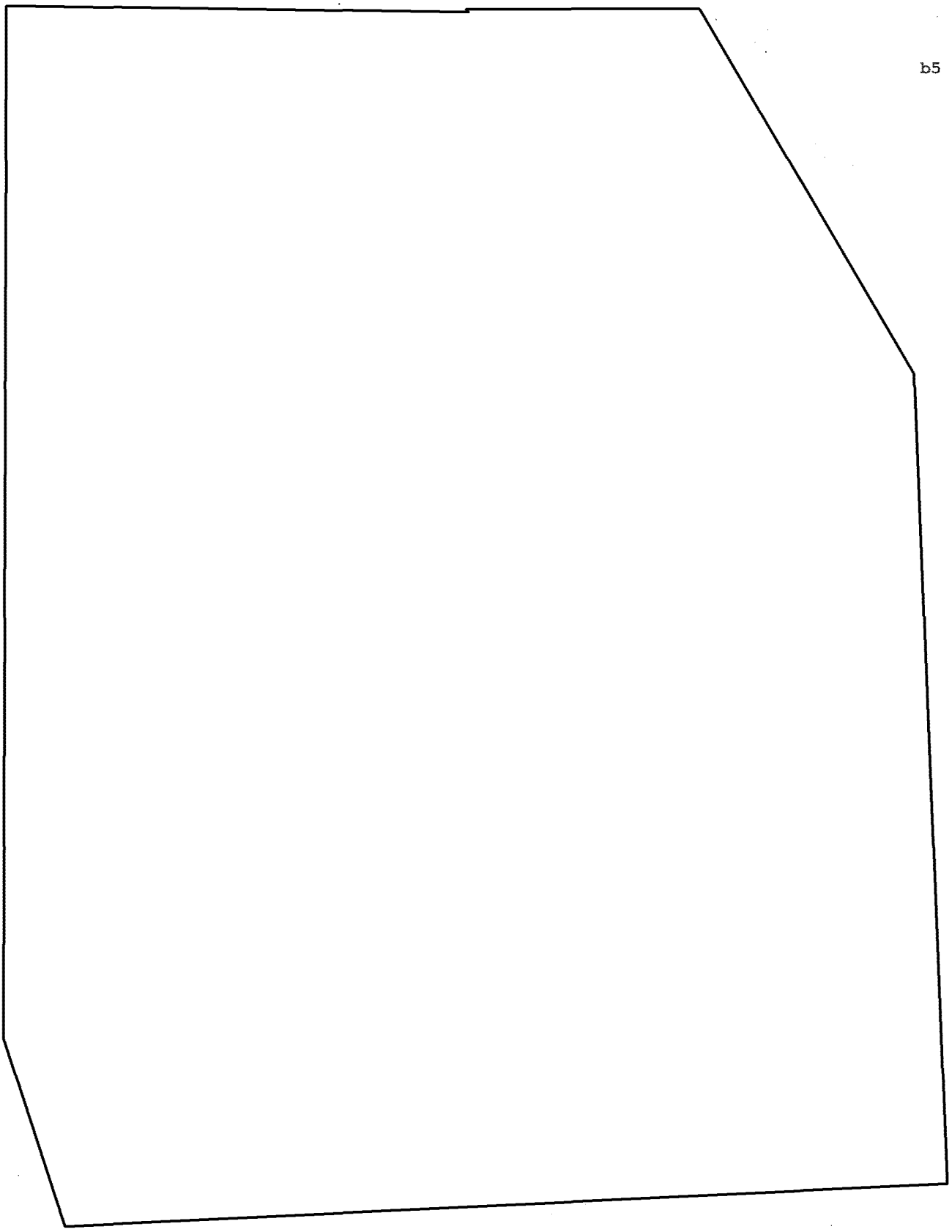
b5

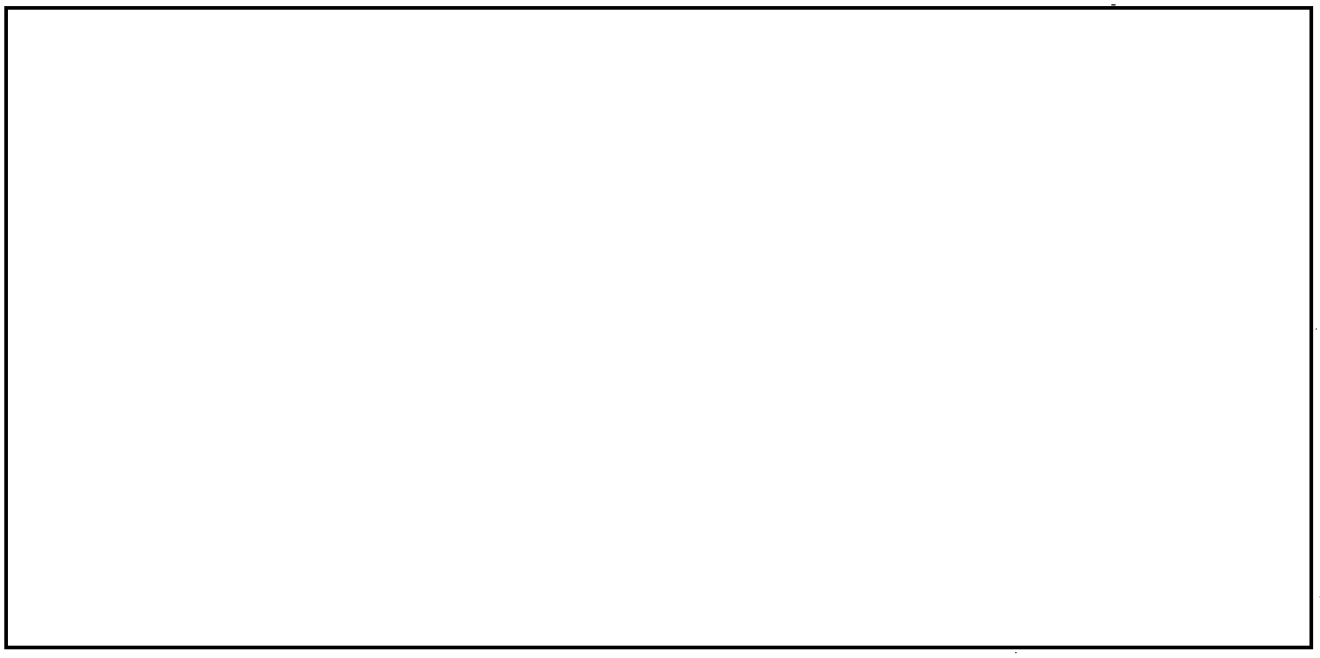


b2
b5
b6
b7C



b5





b5
b6
b7C

~~SECRET~~

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

b1
b6
b7C
b7D

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 08-24-2005
CLASSIFIED BY 65179/DMH/JW/05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 08-24-2030

[redacted] (S)

DATE

b6
b7C
b7D

RE: Request for Emergency Access to Information

Dear [redacted]

b1
b2
b6
b7C
b7D
b7E

Pursuant to Title 18 U.S.C. §2702(b)(8)and §2702(c)(4), the Federal Bureau of Investigation (FBI) requests tha[redacted] (S)

[redacted] (S)

This information should include[redacted]

b2
b7E

By way of background, [provide some information to the service provider that would enable them to reach the conclusion that this involves an emergency to human life or serious physical injury].

b1
b2
b7D
b7E

In an effort to respond to this emergency condition[redacted] requested to provide the above listed information. Authority fo[redacted] o disclose this information to the FBI under the current circumstances rests in 18 U.S.C. § 2702(b)(8), which permits a service provider to voluntarily disclose the content of communications to the FBI "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." See also 18 U.S.C. § 2702(c)(4) which addresses a similar standard for the disclosure of records.

Due to the emergency circumstances surrounding this request, please provide the requested information to Special Agent [Name], [Field Office], [address], [telephone], [facsimile and/or e-mail address] as soon as possible. Any questions can be directed to [name] at [phone #].

Sincerely,

~~SECRET~~

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 08/12/03

To:	All Divisions	**Attn:**	SAC CDC FBIHQ, Manuals Desk
	All Legats	**Attn:**	Legat
	Counterterrorism	**Attn:**	Acting AD John S. Pistole
	Criminal Investigative	**Attn:**	AD Grant D. Ashley
	Cyber	**Attn:**	AD Jana D. Monroe DAD James E. Farnan

From: Office of the General Counsel
Investigative Law Unit/Room 7326
Contact: [redacted]

Approved By: Kelley Patrick W. [redacted] b2 b6

Drafted By: [redacted] b7C

Case ID #: 66F-HQ-1085160 (Pending)
66F-HQ-C1384970

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179/DMH/JW/05-CV-0845

Title: Emergency Disclosures under
18 U.S.C. § 2702
Reporting Requirement

Synopsis: This EC reminds investigative offices of their duty to report all disclosures of a communications content received from service providers (including Internet service providers) between June 11 and August 15, 2003 under the emergency disclosure provision by August 28, 2003.

Reference: 66F-HQ-1085160 Serial 60

Details: Under the emergency disclosure provision, codified at 18 U.S.C. § 2702(b)(7), a service provider can voluntarily provide law enforcement with the content of e-mail or other electronic communications if the service provider reasonably believes that there is an emergency involving death or serious physical injury which requires immediate action. Congress created a reporting requirement in the Homeland Security Act which requires the government to report to the DOJ within 90 days of receipt of a disclosure of a communication's content. The above referenced EC discusses the reporting requirement in detail.

In order to comply with this statutory reporting requirement, all disclosures of a communication's content received from a service provider under this provision during the period

b2
b7E

between June 11 and August 15, 2003, should be reported to the Investigative Law Unit (ILU), Office of the General Counsel by August 28, 2003. [redacted]

This reporting should be done by: 1) either sending an e-mail message or telephonically notifying Assistant General Counsel (AGC) [redacted] ILU, OGC at [redacted] or [redacted] ILU, OGC [redacted] as soon as possible that an office will be submitting a report; and 2) submitting the information detailed in the above referenced EC (the date of disclosure and the number of messages where the content of the message was received with a separate line item for each subscriber identity) to ILU by August 28, 2003 so that any necessary reporting can be made to the DOJ within the statutory deadlines. Negative reporting is not required.

b2
b6
b7C

Any questions should be directed to AGC [redacted] at telephone number [redacted] or [redacted] at [redacted]

b2
b6
b7C

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Any office that has received the content of an electronic communication from a service provider under the emergency disclosure provision in 18 U.S.C. § 2702(b)(7) between June 11 and August 15, 2003 should immediately notify the Investigative Law Unit either telephonically or via e-mail and provide the necessary reporting by August 28, 2003.

CC: 1 - Kelley
1 - [redacted]
1 -
2 - ILU

b6
b7C

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

DRAFT

Precedence: IMMEDIATE **Date:** 04/15/2003

To: All Field Offices **Attn:** ADIC
SAC
CDC

From: Office of the General Counsel
Investigative Law Unit/Room
Contact: [redacted] x[redacted] b2 b6 b7C

Approved By: Kelley Patrick W
[redacted]

Drafted By: [redacted]

Case ID #: 66F-HQ-1085160 (Pending)
66F-HQ-1085159 (Pending)
66F-HQ-C1382989 (Pending)
66F-HQ-C1384970

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179/DMH/JW/05-CV-0845

Title: Emergency Disclosures under ECPA
18 U.S.C. § 2702
Reporting Requirement

Synopsis: This EC advises receiving field offices of the reporting requirement under 18 U.S.C. Section 2702(b)(7) regarding any voluntary disclosures made by a service provider to the FBI under this emergency disclosure provision. Field offices must immediately report if they received any voluntary disclosures of content or records from service providers under this provision between January 24, 2003 and March 31, 2003. Negative reports are not required. Additional reports will be required at later dates.

Enclosure(s): Sample report b2

Details: The Electronic Communications Privacy Act (ECPA), codified in 18 U.S.C. § 2701, *et. seq.*, provides privacy protection for electronic communications, such as e-mail, and associated records. It also outlines the compulsory process that law enforcement can use to obtain both the content of communications and records held by an electronic communications service provider or a remote computing service, [redacted] The USA Patriot Act created a voluntary disclosure provision which explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. 18 U.S.C. § 2702(b)(7); 18 U.S.C. § 2702(c)(4). The Homeland Security Act modified this provision and created a reporting requirement for every disclosure made under this provision. b7E

This EC provides guidance on the reporting requirement and notifies the field of urgent deadlines in order to ensure full compliance with the statutory deadlines. Further guidance will be issued in the near future on the use of the provision.

The reporting requirement as enacted in the Homeland Security Act reads as follows:

> "A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act."[1]

While the language of the reporting requirement states that any disclosure to the government under 18 U.S.C. § 2702(b) must be reported, a reasonable interpretation of the legislative history narrows this reporting requirement to 2702(b)(7), the emergency disclosure provision.[2] This is a one-time reporting requirement, meaning that after the Attorney General files the report in November 2003, the reporting requirement ceases.

[redacted] b2 b7E

[redacted] In the cover letter to the report we will explain what the data means and why we

[1]Homeland Security Act of 2002, P.L.107-296, § 225(d)(2).

[2]§ 2702(b) authorizes the ISP to make disclosures to the intended recipient of the e-mail, consistent with the consent of the originator or recipient, and to another service used to forward the mail to the intended recipient. Congress did not intend for the Attorney General to report to Congress every time that a government employee receives an e-mail that was forwarded through an ISP. The legislative history demonstrates that Congress' concern was that law enforcement might abuse the ability to approach an ISP and present emergency circumstances to the ISP, causing the ISP to voluntarily provide e-mail content and records to the law enforcement agency. It is only in this context that the reporting requirement is discussed in the legislative history. See H.R. Rep. 107-497, pg. 14; 148 Cong. Rec. H4580-05, pg. H4583 (Congressional debate on the Cyber Security Enhancement Act of 2002, dated July 15, 2002)(statement of Ms. Jackson-Lee).

cannot report the exact information requested. By reporting and explaining this information, the FBI will be complying with the intent of the law.

To facilitate the reporting process, the Investigative Law Unit (ILU), Office of the General Counsel (OGC) will act as the central point for all FBI reports of disclosures under the emergency disclosure provision. Field offices should provide ILU with a list of the disclosures they have received under this provision. Information should be submitted in the form of an Excel spreadsheet with one column each for the following information: 1) the date of receipt of the disclosure; 2) whether content (i.e., e-mail) or records were received; and 3) the number of e-mail messages or communications disclosed. A separate record or line item should be listed for each account or identity about which the disclosure was made. A sample spreadsheet is attached.

The statute requires that disclosures made under this emergency disclosure provision are to be reported to the Attorney General within 90 days of the disclosure. As a part of the Homeland Security Act, the reporting requirement became effective on January 24, 2003. Therefore, any disclosures received prior to January 24, 2003, need not be reported. Any disclosures made under § 2702(b)(7) and received on January 24, 2003, must be reported to the Department of Justice (DOJ) by April 24, 2003. In order to provide this information to the DOJ within the deadline, any office which received disclosures under this emergency disclosure provision between January 24 and March 31, 2003 are to: 1) telephonically notify Assistant General Counsel (AGC) [redacted] ILU, OGC at [redacted] or [redacted] ILU, OGC [redacted] as soon as possible; and 2) submit the above detailed information to ILU by April 21, 2003 so that any necessary reporting can be made to the DOJ within the statutory deadlines. Negative reporting is not required.

b2
b6
b7C

Thereafter, reports should be submitted quarterly (via EC with an electronic copy also sent via e-mail) under the following schedule: all disclosures received between April 1 and June 10, 2003 are to be reported to ILU by June 20, 2003; all disclosures received between June 11 and August 15, 2003 are to be submitted to ILU by August 31, 2003; all disclosures received between August 16 and October 15, 2003 are to be submitted to ILU by November 1, 2003.

Any questions should be directed to AGC [redacted] at telephone number [redacted] or [redacted] at [redacted]

b2
b6
b7C

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Any office which has received a disclosure of electronic communications or records from a service provider under 18 U.S.C. § 2702 since January 24, 2003 are to telephonically notify the above contact person immediately and provide a written report of such disclosures in accordance with the dates specified above. Negative reports are not required.

♦♦

cc: 1 - Mr. Kelley
1 - Mr. Steele
1 -
1 -
1 -
1 -
1 -
1 -
1 -
1 -
2 - ILU Files

b6
b7C

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/30/2003 DRAFT

To:	All Divisions	**Attn:**	SAC CDC FBIHQ, Manuals Desk
	All Legats	**Attn:**	Legat
	Counterterrorism	**Attn:**	AD Larry A. Mefford
	Criminal Investigative	**Attn:**	AD Grant D. Ashley
	Cyber	**Attn:**	AD Jana D. Monroe DAD James E. Farnan

From: Office of the General Counsel
Investigative Law Unit/Room 7326
Contact: [redacted] b2 b6 b7C

Approved By: Rowan J Patrick [redacted]

Drafted By: [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179/DMH/JW/05-CV-0845

Case ID #: 66F-HQ-1085160 (Pending)
66F-HQ-C1384970

Title: Emergency Disclosures under
18 U.S.C. § 2702
Reporting Requirement

Synopsis: This EC reminds investigative offices of their duty to report all disclosures of a communications content received from service providers, including Internet service providers, under the emergency disclosure provision codified at 18 U.S.C. § 2702(b)(7) by June 20, 2003.

Reference: 66F-HQ-1085160 Serial 60

Enclosure(s): Sample Report Format

Details: Under the emergency disclosure provision, codified at 18 U.S.C. § 2702(b)(7), a service provider can voluntarily provide law enforcement with the content of e-mail or other electronic communications if the service provider reasonably believes that there is an emergency involving death or serious physical injury which requires immediate action. Congress created a reporting requirement in the Homeland Security Act which requires the government to report to the DOJ within 90 days of receipt of a disclosure of a communication's content. The above referenced EC discusses the reporting requirement in detail.

b2
b7E

In order to comply with this statutory reporting requirement, all disclosures of a communication's content received from a service provider under this provision during the period between April 1 and June 10, 2003, should be reported to the Investigative Law Unit (ILU) Office of the General Counsel by June 20, 2003 [redacted]

This reporting should be done by: 1) either sending an e-mail message or telephonically notifying Assistant General Counsel (AGC) [redacted] ILU, OGC at [redacted] or [redacted] ILU, OGC [redacted] as soon as possible that an office will be submitting a report; and 2) submitting the information detailed in the above referenced EC (the date of disclosure and the number of messages where the content of the message was received with a separate line item for each subscriber identity) to ILU by June 20, 2003 so that any necessary reporting can be made to the DOJ within the statutory deadlines. Negative reporting is not required.

b2
b6
b7C

Any questions should be directed to AGC [redacted] at telephone number [redacted] or [redacted] at [redacted]

b2
b6
b7C

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Any office that has received the content of an electronic communication from a service provider under the emergency disclosure provision in 18 U.S.C. § 2702(b)(7) between April 1 and June 10, 2003 should immediately notify the Investigative Law Unit either telephonically or via e-mail and provide the necessary reporting by June 20, 2003.

CC: 1 - Rowan
1 - [redacted]
1 - [redacted]
2 - ILU

b6
b7C

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

DRAFT

Precedence: ROUTINE **Date:** 10/7/03

To:	All Divisions	**Attn:**	SAC CDC FBIHQ, Manuals Desk
	All Legats	**Attn:**	Legat
	Counterterrorism	**Attn:**	AD John S. Pistole
	Criminal Investigative	**Attn:**	AD Grant D. Ashley
	Cyber	**Attn:**	AD Jana D. Monroe DAD James E. Farnan

From: Office of the General Counsel
Investigative Law Unit/Room 7326
Contact: [redacted]

Approved By: Kelley Patrick W. [redacted]

Drafted By: [redacted]

b2
b6
b7C

Case ID #: 66F-HQ-1085160 (Pending)
66F-HQ-C1384970

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179/DMH/JW/05-CV-0845

Title: Emergency Disclosures under
18 U.S.C. § 2702
Reporting Requirement

Synopsis: This EC reminds investigative offices of their duty to report all disclosures of a communication's content received from service providers (including Internet service providers) between August 16 and October 15, 2003 under the emergency disclosure provision by October 24, 2003.

Reference: 66F-HQ-1085160 Serial 60

Details: Under the emergency disclosure provision, codified at 18 U.S.C. § 2702(b)(7), a service provider can voluntarily provide law enforcement with the content of e-mail or other electronic communications if the service provider reasonably believes that there is an emergency involving death or serious physical injury which requires immediate action. Congress created a reporting requirement in the Homeland Security Act which requires the government to report to the DOJ within 90 days of receipt of a disclosure of a communication's content. The above referenced EC discusses the reporting requirement in detail.

In order to comply with this statutory reporting requirement, all disclosures of a communication's content received from a service provider under this provision during the period

b2
b7E

between August 16 and October 15, 2003, should be reported to the Investigative Law Unit (ILU), Office of the General Counsel by October 24, 2003. [redacted]

This reporting should be done by: 1) either sending an e-mail message or telephonically notifying Assistant General Counsel (AGC) [redacted] ILU, OGC at [redacted] or [redacted] ILU, OGC [redacted] as soon as possible that an office will be submitting a report; and 2) submitting the information detailed in the above referenced EC (the date of disclosure and the number of messages where the content of the message was received with a separate line item for each subscriber identity) to ILU by October 24, 2003 so that any necessary reporting can be made to the DOJ within the statutory deadlines. Negative reporting is not required.

b2
b6
b7C

Any questions should be directed to AGC [redacted] at telephone number [redacted] or [redacted] at [redacted]

b2
b6
b7C

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Any office that has received the content of an electronic communication from a service provider under the emergency disclosure provision in 18 U.S.C. § 2702(b)(7) between August 16 and October 15, 2003 should immediately notify the Investigative Law Unit either telephonically or via e-mail and provide the necessary reporting by October 24, 2003.

CC: 1 - Kelley
1 - [redacted]
1 - [redacted]
2 - ILU

b6
b7C

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

DRAFT

Precedence: IMMEDIATE **Date:** 05/27/2003

To: All Legats **Attn:** Legat

Criminal Investigative **Attn:** AD Grant D. Ashley

Cyber **Attn:** AD Jana D. Monroe
DAD James E. Farnan

Counterterrorism **Attn:** AD Larry A. Mefford

b2
b6
b7C

From: Office of the General Counsel
Investigative Law Unit/Room 7326
Contact:

Approved By: Rowan J. Patrick

Drafted By:

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179/DMH/JW/05-CV-0845

Case ID #: 66F-HQ-1085160

Title: Emergency Disclosures under ECPA
18 U.S.C. 2702
Reporting Requirement

Synopsis: To advise the Legats and several HQ divisions of the requirement to immediately report to the Office of the General Counsel any disclosures of e-mail content made by a service provider to the FBI between the dates of January 24 and March 31, 2003 in accordance with the emergency disclosure provision of the Electronic Communication Privacy Act (ECPA), 18 U.S.C. § 2702(b)(7).

Reference: 66F-HQ-1085160 Serial 60

Details: The above referenced EC was sent to all field offices to advise on a new reporting requirement established in the Homeland Security Act for any emergency disclosures of the content of an electronic communication by a service provider under 18 U.S.C. 2702(b)(7). It further notified the field of urgent deadlines in order to ensure full compliance with the statutory deadlines.

Further guidance will be issued in the near future on the use of the provision.

The Electronic Communications Privacy Act (ECPA), codified in 18 U.S.C. § 2701, et. seq., provides privacy protection for electronic communications, such as e-mail and associated records. It also outlines the compulsory process that law enforcement can use to obtain both the content of communications and records held by an electronic communications service provider or a remote

b2
b7E

b2
b7E

computing service. [redacted] The USA Patriot Act created a voluntary disclosure provision which explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. 18 U.S.C. § 2702(b)(7); 18 U.S.C. § 2702(c)(4). The Homeland Security Act modified this provision and created a reporting requirement for every disclosure of a communication's content made under this provision. The reporting requirement as enacted in the Homeland Security Act reads as follows:

> "A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act."[1]

While the language of the reporting requirement states that any disclosure to the government under 18 U.S.C. § 2702(b) must be reported, a reasonable interpretation of the legislative history narrows this reporting requirement to 2702(b)(7), the emergency disclosure provision.[2] This is a one-time reporting requirement, meaning that after the Attorney General files the report in November 2003, the reporting requirement ceases.

[redacted]

[1]Homeland Security Act of 2002, P.L.107-296, § 225(d)(2).

b2
b7E

[redacted]

b5

b2
b7E

In the cover letter to the report we will explain what the data means and why we cannot report the exact information requested. By reporting and explaining this information, the FBI will be complying with the intent of the law.

To facilitate the reporting process, the Investigative Law Unit (ILU), Office of the General Counsel (OGC) will act as the central point for all FBI reports of disclosed content under the emergency disclosure provision. Offices in receipt of such disclosures should provide ILU with a list of the disclosures of content they have received under this provision. Information should be submitted in the form of an Excel spreadsheet with one column each for the following information: 1) the date of receipt of the disclosure, and 2) the number of e-mail messages or communications disclosed by the service provider (not the number of e-mail accounts, but the actual number of e-mail messages which were received for each account). A separate record or line item should be listed for each account or identity about which the disclosure was made.

The statute requires that disclosures made under this emergency disclosure provision are to be reported to the Attorney General within 90 days of the disclosure. As a part of the Homeland Security Act, the reporting requirement became effective on January 24, 2003. Therefore, any disclosures received prior to January 24, 2003 need not be reported. The first report to DOJ was submitted on April 25, 2003. Therefore, at this time, OGC seeks the immediate reporting of any disclosures made to any Legat or other FBI entity between January 24 and March 31, 2003. This reporting should be done by: 1) telephonically notifying Assistant General Counsel (AGC) ILU, OGC at or ILU, OGC as soon as possible; and 2) submitting the above detailed information to ILU so that any necessary reporting can be made to the DOJ within the statutory deadlines. Negative reporting is not required.

b2
b6
b7C
b7E

Thereafter, reports should be submitted quarterly (via EC with an electronic copy also sent via e-mail) under the following schedule: all disclosures received between April 1 and June 10, 2003 are to be reported to ILU by June 20, 2003; all disclosures received between June 11 and August 15, 2003 are to be submitted to ILU by August 31, 2003; all disclosures received between August 16 and October 15, 2003 are to be submitted to ILU by November 1, 2003.

Any questions should be directed to AGC at telephone number or at

b2
b6
b7C

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Any office that has received a disclosure of the content of an electronic communication from a service provider under the emergency disclosure provision in 18 U.S.C. § 2702(b)(7) between January 24 and March 31, 2003 should immediately notify the Investigative Law Unit telephonically and provide the necessary reporting as soon as possible.

CC: [redacted]
ILU Files

b6
b7C

♦♦

May 22, 2003

Ms. Maureen Killion
Director
Office of Enforcement Operations
Department of Justice
1301 New York Avenue, N.W.
Washington, D.C. 20005

RE: 18 U.S.C. § 2702 Reporting Requirement

Dear Ms. Killion:

This report supplements the initial report submitted to your office on April 25, 2003 detailing disclosures received by the FBI from service providers under the emergency disclosure provision found in 18 U.S.C. § 2702(b)(7).

Should there be any questions in regard to this report, please contact [redacted] Assistant General Counsel of my office at [redacted]

b2
b6
b7C

Sincerely,

J. Patrick Rowan
Acting Deputy General Counsel
Office of the General Counsel

cc: [redacted]

1 - Mr. Kelley
1 - Mr. Rowan
1 - Mr. Steele
1 - [redacted]
1 - [redacted]
1 - [redacted]
2 - ILU
1 - 66F-HQ-1085160
1 - 66F-HQ-A1085154 - Admin

b6
b7C

~~SECRET~~

DATE: 12-13-2005
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845
REASON: 1.4 (c)
DECLASSIFY ON: 12-13-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Amendment to Report of Disclosures Received by the FBI Under the Emergency Disclosure Provision 18 U.S.C. § 2702(b)(7) Between January 24 and March 31, 2003

On April 25, 2003, the FBI submitted a report to the Office of Enforcement Operations at the Department of Justice listing the disclosures received by the FBI under the emergency disclosure provision of the Electronic Communications Privacy Act, codified at 18 U.S.C. § 2702(b)(7), during the period of January 24 and March 31, 2003 in order to comply with the reporting requirement established in the Homeland Security Act (P.L. 107-296 § 225(d)(2)). This provision requires that the FBI report to the DOJ certain specified information for each occurrence where a service provider voluntarily discloses to the FBI the content of a communication (i.e., e-mail content) in order to respond to an emergency. Such reporting is to be done within 90 days of the FBI's receipt of the disclosure.

This document supplements the report filed on April 25 with several additional disclosures that were recently identified. Each line item listed in this report reflects the disclosures made on that date pertaining to a specific identity. One subscriber may have multiple on-line identities or accounts. The FBI may not be able to distinguish accounts and identities from customers and subscribers until well into the investigation [redacted] (S)

b1
b2
b7E

The following attachment lists the date for each disclosure and the number of messages received that pertain to each separate identity. Each line item represents a separate identity as described above. The number of communications disclosed includes spam e-mail messages (unsolicited "junk" advertisements) and delivery notification messages (messages automatically generated by the system to notify the originator of the delivery status of a message, i.e., "e-mail not sent due to system failure.")

~~SECRET~~

Disclosures Received
by the FBI
Under the Emergency Disclosure Provision
18 U.S.C. § 2702
Between April 1 and June 10, 2003

The Homeland Security Act, P.L. 107-296, established a reporting requirement for disclosures received under the emergency disclosure provision codified at 18 U.S.C. § 2702(b). P.L. 107-296 § 225 (d)(2). In accordance with this provision, the FBI provides the following report of disclosures received under 18 U.S.C. § 2702(b)(7).

The reporting requirement as enacted in the Homeland Security Act reads as follows:

> "A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act."[1]

The FBI worked with the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice to appropriately interpret this statutory language in order to provide the information sought by Congress to the Department of Justice. CCIPS and the FBI concur that the Congressional intent of this provision was to establish a reporting requirement for emergency disclosures of content made under 18 U.S.C. § 2702(b)(7), as opposed to all disclosures made under 18 U.S.C. § 2702(b). 18 U.S.C. § 2702(b) authorizes a service provider to make disclosures under various circumstances including, among others, disclosures to the intended recipient of the e-mail, disclosures to another service provider in order to forward the mail to the intended recipient, and disclosures consistent with the consent of the originator or recipient. Congress did not intend for the Attorney General to report to Congress every time that a government employee receives an e-mail that was forwarded through the Internet. The legislative history demonstrates that Congress was concerned the government might abuse the ability to obtain information under the emergency disclosure provision found in 18 U.S.C. § 2702(b)(7). It is only in this context that the reporting requirement is discussed in the legislative history. See H.R. Rep. 107-497, pg. 14; 148 Cong. Rec. H4580-05, pg. H4583 (Congressional debate on the Cyber Security Enhancement Act of 2002, dated July 15, 2002)(statement of Ms. Jackson-Lee). Thus, all the disclosures reported in this document were emergency disclosures of content made under 18 U.S.C. § 2702(b)(7).

Each line item listed in this report reflects the disclosures made on that date pertaining to

[1]Homeland Security Act of 2002, P.L.107-296, § 225(d)(2).

a specific identity. One subscriber may have multiple on-line identities or accounts. The FBI may not be able to distinguish accounts and identities from customers and subscribers until well into the investigation.

(S)

b1
b2
b7E

The following attachment lists the date for each disclosure and the number of messages received that pertain to each separate identity. Each line item represents a separate identity as described above.

b2
b7E

The number of communications disclosed includes spam e-mail messages (unsolicited "junk" advertisements) and delivery notification messages (messages automatically generated by the system to notify the originator of the delivery status of a message, i.e., "e-mail not sent due to system failure.")

Legal Issues to Recognize

[redacted]

Assistant General Counsel

Office of the General Counsel

[redacted]

b2

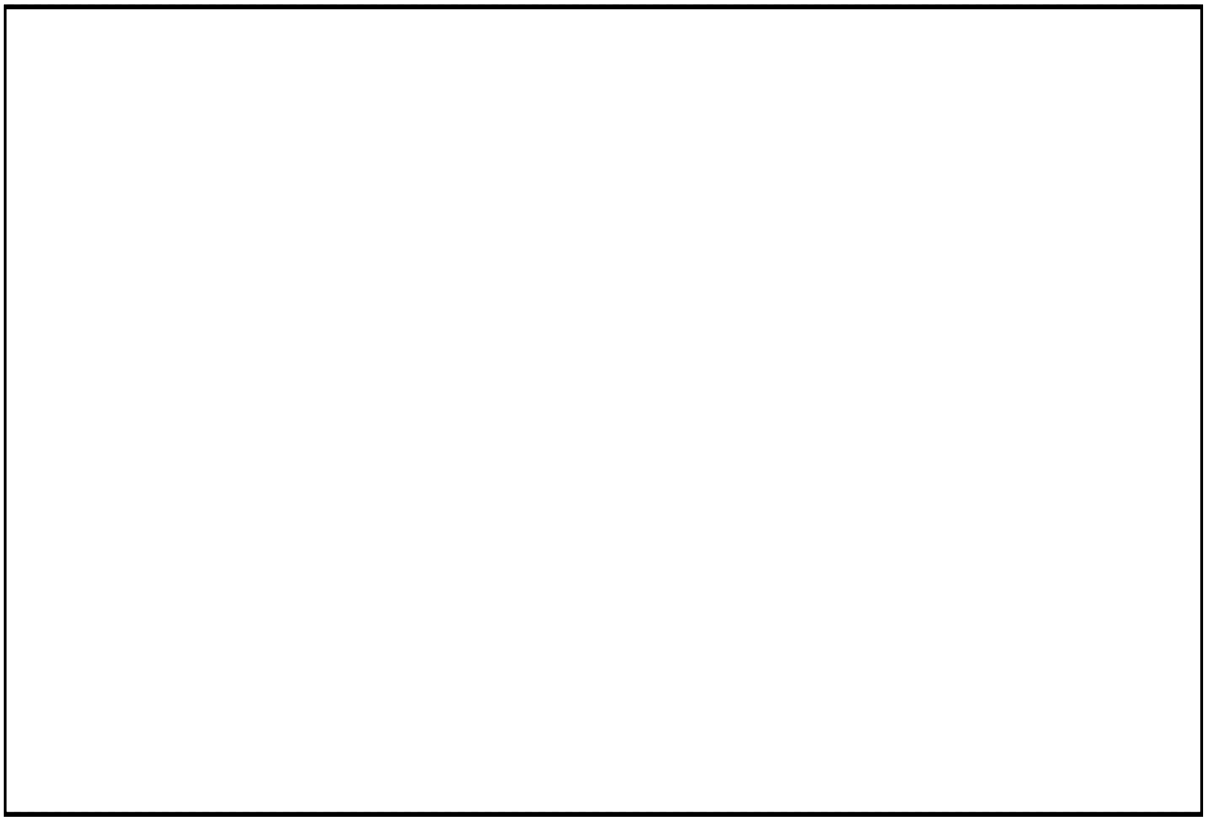
b6

b7C

3) Helpful Service Providers

b2

b7E



b5

Helpful Service Providers – cont.

b5

-
-

Remedies

- [redacted]
- [redacted]

b5

Legal Issues

b6
b7C

Office of the General Counsel

- Patriot Act
- Case Law Update
- On-Line Guidelines - Update
- UC contacts in On-Line Environment

Patriot Act - ECPA

Nationwide Search Warrants for E-mail

– Past - multiple jurisdictions often involved.

– Governed by Sunset Provision - December 31, 2005.

18 USC 2703

Patriot Act - ECPA

Voluntary Disclosures by ISP

- Emergency Disclosures

  Std: immediate risk of death or serious physical injury to any person

- Self - protection
  - non-content records
  - content previously covered

- Sunset provision applies

18 USC 2702(b)(6)

Patriot Act - ECPA

Voice Mail

- 18 USC 2703 now applies
  - D-order
  - Search Warrant

- Change to definition of wire communication.

18 USC 2510

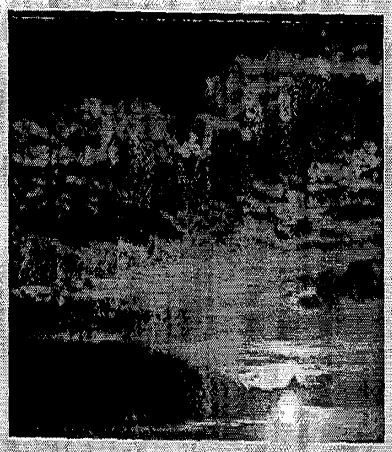
USA Patriot Act

[redacted]

b6
b7C

Office of the General Counsel
Federal Bureau of Investigation

Sunset Provisions



- Many investigative tools set to expire on December 31, 2005 unless Congress renews them.

- Need to collect good examples on proper and effective use of these tools. (Send examples to CDC or OGC)

Single Jurisdiction for Search Warrants

- Limited to international and domestic terrorism investigations
- Provides court in a district where terrorism related activities have occurred the authority to issue search warrants for persons and/or property located in other districts.
- Check with DOJ TVCS first

(Rule 41(a))

Nationwide Search Warrants for E-mail

- Applies to all criminal investigations.
- Past - multiple jurisdictions often involved.
- Governed by Sunset Provision - December 31, 2005.

18 USC § 2703

FISA Changes

- Change in "primary purpose" standard for FISA – now "significant purpose."
- Roving FISA authority
- Extended standard duration for several categories of FISA orders.

FISA Changes (cont.)

- Reduced showing required for
  - pen register/trap and trace authority.
  - business records.
- Increased civil liability for unauthorized disclosures.
- Immunity from civil liability for compliance with FISA.
- Obligation to disclose foreign intell to Director Central Intelligence.

Voluntary Disclosures by ISP

- Emergency Disclosures
  - Std: immediate risk of death or serious physical injury to any person
- Self - protection
  - non-content records
  - content previously covered
- Sunset provision applies

18 USC § 2702(b)(6)

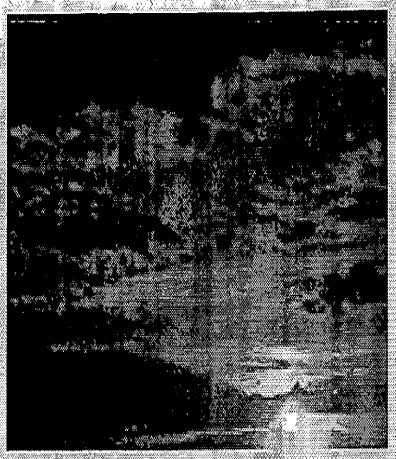
Nationwide Search Warrants for E-mail

- Past - multiple jurisdictions often involved.

- Governed by Sunset Provision - December 31, 2005.

18 USC § 2703

Sunset Provisions



- Many investigative tools set to expire on December 31, 2005 unless Congress renews them.

- Need to collect good examples on proper and effective use of these tools. (Send examples to CDC or OGC)

Nationwide Search Warrants for E-mail

- Applies to all criminal investigations.
- Past - multiple jurisdictions often involved.
- Governed by Sunset Provision - December 31, 2005.

18 USC § 2703

FISA Changes

- Change in "primary purpose" standard for FISA – now "significant purpose."
- Roving FISA authority
- Extended standard duration for several categories of FISA orders.

FISA Changes (cont.)

- Reduced showing required for
  - pen register/trap and trace authority.
  - business records.
- Increased civil liability for unauthorized disclosures.
- Immunity from civil liability for compliance with FISA.
- Obligation to disclose foreign intell to Director Central Intelligence.

Voluntary Disclosures by ISP

- Emergency Disclosures
  - Std: immediate risk of death or serious physical injury to any person
- Self - protection
  - non-content records
  - content previously covered
- Sunset provision applies

18 USC § 2702(b)(6)

Monitoring Computer Trespassers

- Amended T-3 to allow victims to invite law enforcement to monitor a hacker's comms in a protected computer.
- Requires:
  - Consent by owner
  - Must have ongoing investigation.
  - Reasonable belief that content relevant
  - Only for comms to/from hackers
- Violation of contract terms (I.e. spammers) not sufficient to use this exception.

- Voice Mail – obtained with a §2703 D-order or search warrant.
- Educational Records for terrorism cases – AAG approval
- DNA predicates include terrorism related offenses

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 178
Page 29 ~ Duplicate
Page 30 ~ Duplicate
Page 31 ~ Duplicate
Page 32 ~ Duplicate
Page 33 ~ Duplicate
Page 34 ~ Duplicate
Page 35 ~ Duplicate
Page 36 ~ Duplicate
Page 37 ~ Duplicate
Page 38 ~ Duplicate
Page 39 ~ Duplicate
Page 40 ~ Duplicate
Page 41 ~ Duplicate
Page 42 ~ Duplicate
Page 43 ~ Duplicate
Page 44 ~ Duplicate
Page 45 ~ Duplicate
Page 46 ~ Duplicate
Page 47 ~ Duplicate
Page 48 ~ Duplicate
Page 49 ~ Duplicate
Page 50 ~ Duplicate
Page 51 ~ Duplicate
Page 52 ~ Duplicate
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 55 ~ Duplicate
Page 56 ~ Duplicate
Page 57 ~ Duplicate
Page 58 ~ Duplicate
Page 59 ~ Duplicate
Page 60 ~ Duplicate
Page 61 ~ Duplicate
Page 62 ~ Duplicate
Page 63 ~ Duplicate
Page 64 ~ Duplicate
Page 65 ~ Duplicate
Page 66 ~ Duplicate
Page 67 ~ Duplicate
Page 68 ~ Duplicate
Page 69 ~ Duplicate
Page 70 ~ Duplicate
Page 71 ~ Duplicate
Page 72 ~ Duplicate

Page 73 ~ Duplicate
Page 74 ~ Duplicate
Page 75 ~ Duplicate
Page 76 ~ Duplicate
Page 77 ~ Duplicate
Page 78 ~ Duplicate
Page 79 ~ Duplicate
Page 80 ~ Duplicate
Page 81 ~ Duplicate
Page 82 ~ Duplicate
Page 83 ~ Duplicate
Page 84 ~ Duplicate
Page 85 ~ Duplicate
Page 86 ~ Duplicate
Page 87 ~ Duplicate
Page 88 ~ Duplicate
Page 89 ~ Duplicate
Page 90 ~ Duplicate
Page 91 ~ Duplicate
Page 92 ~ Duplicate
Page 93 ~ Duplicate
Page 100 ~ Duplicate
Page 101 ~ Duplicate
Page 102 ~ Duplicate
Page 103 ~ Duplicate
Page 104 ~ Duplicate
Page 105 ~ Duplicate
Page 106 ~ Duplicate
Page 107 ~ Duplicate
Page 108 ~ Duplicate
Page 109 ~ Duplicate
Page 110 ~ Duplicate
Page 111 ~ Duplicate
Page 112 ~ Duplicate
Page 113 ~ Duplicate
Page 114 ~ Duplicate
Page 115 ~ Duplicate
Page 116 ~ Duplicate
Page 117 ~ Duplicate
Page 118 ~ Duplicate
Page 119 ~ Duplicate
Page 120 ~ Duplicate
Page 121 ~ Duplicate
Page 122 ~ Duplicate
Page 123 ~ Duplicate
Page 124 ~ Duplicate
Page 125 ~ Duplicate
Page 126 ~ Duplicate
Page 127 ~ Duplicate
Page 128 ~ Duplicate
Page 129 ~ Duplicate

Page 130 ~ Duplicate
Page 131 ~ Duplicate
Page 132 ~ Duplicate
Page 133 ~ Duplicate
Page 134 ~ Duplicate
Page 135 ~ Duplicate
Page 136 ~ Duplicate
Page 137 ~ Duplicate
Page 138 ~ Duplicate
Page 139 ~ Duplicate
Page 140 ~ Duplicate
Page 141 ~ Duplicate
Page 142 ~ Duplicate
Page 143 ~ Duplicate
Page 144 ~ Duplicate
Page 145 ~ Duplicate
Page 146 ~ Duplicate
Page 147 ~ Duplicate
Page 148 ~ Duplicate
Page 149 ~ Duplicate
Page 150 ~ Duplicate
Page 151 ~ Duplicate
Page 152 ~ Duplicate
Page 153 ~ Duplicate
Page 154 ~ Duplicate
Page 155 ~ Duplicate
Page 156 ~ Duplicate
Page 157 ~ Duplicate
Page 158 ~ Duplicate
Page 159 ~ Duplicate
Page 160 ~ Duplicate
Page 161 ~ Duplicate
Page 162 ~ Duplicate
Page 163 ~ Duplicate
Page 164 ~ Duplicate
Page 165 ~ Duplicate
Page 242 ~ Duplicate
Page 243 ~ Duplicate
Page 244 ~ Duplicate
Page 245 ~ Duplicate
Page 246 ~ Duplicate
Page 247 ~ Duplicate
Page 248 ~ Duplicate
Page 251 ~ Duplicate
Page 267 ~ Referral/Direct
Page 268 ~ Referral/Direct
Page 269 ~ Referral/Direct
Page 270 ~ Referral/Direct
Page 271 ~ Referral/Direct
Page 272 ~ Referral/Direct
Page 273 ~ Referral/Direct

Page 274 ~ Referral/Direct
Page 275 ~ Referral/Direct
Page 276 ~ Referral/Direct
Page 277 ~ Referral/Direct
Page 278 ~ Referral/Direct
Page 279 ~ Referral/Direct
Page 280 ~ Referral/Direct
Page 281 ~ Referral/Direct
Page 282 ~ Referral/Direct
Page 285 ~ Referral/Direct
Page 286 ~ Referral/Direct
Page 292 ~ Referral/Direct
Page 293 ~ Referral/Direct
Page 315 ~ Duplicate
Page 316 ~ Duplicate
Page 317 ~ Duplicate
Page 318 ~ Duplicate
Page 319 ~ Duplicate
Page 320 ~ Duplicate
Page 321 ~ Duplicate
Page 322 ~ Duplicate
Page 323 ~ Duplicate
Page 324 ~ Duplicate
Page 325 ~ Duplicate
Page 326 ~ Duplicate
Page 327 ~ Duplicate
Page 328 ~ Duplicate
Page 329 ~ Duplicate
Page 330 ~ Duplicate
Page 331 ~ Duplicate
Page 332 ~ Duplicate
Page 333 ~ Duplicate

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

05-CV-0845

Precedence: IMMEDIATE **Date:** 10/10/2003

To: All Divisions **Attn:** ADIC, AD, DAD, SAC, CDC

From: Office of the General Counsel
National Security Law Branch
Contact: [redacted] b2 b6

Approved By: Mueller Robert S III b7C

Drafted By: [redacted] b6 b7C

Case ID #: 66F-HQ-A1431182

Title: BUSINESS RECORD APPLICATIONS
DELEGATION OF AUTHORITY

Synopsis: Delegates signature authority for Applications for Business Records to FBIHQ officials under 50 U.S.C. § 1861.

Details: The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C § 1861, provides for access to certain business records for foreign intelligence (FI) and international terrorism (IT) investigations through issuance of an order from the FISA Court (FISC). Section 1861(a) authorizes the "Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge)" to make an application for the order.

Thus, as permitted by 50 U.S.C. § 1861(a), I hereby designate certification signature authority for applications for FISA business records to the following FBI Officials:

1. The Deputy Director;

2. The Executive Assistant Director for Counterterrorism/Counterintelligence;

3. The Assistant Director and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; and

4. The General Counsel, the Deputy General Counsel for National Security Affairs, and the Senior Counsel for National Security Affairs.

The National Security Law Branch is hereby authorized to prepare business record applications and will issue guidance on the application process.

LEAD:

Set Lead 1: (adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in CI and IT operations and to other personnel as appropriate.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 10/29/2003

To: All Field Offices **Attn:** ADIC;
SAC;
CDC
CI/CT Supervisors
AD Pistole;
DADs;
Section Chiefs

Counterterrorism

Counterintelligence AD Szady;
DADs;
Section Chiefs

05-CV-0845

From: General Counsel
National Security Law Unit, Room 7975
Contact: [redacted] b2 b6 b7C

Approved By: Caproni Valerie E [redacted] b6 b7C

Drafted By: [redacted] pik b7C

Case ID #: 66F-HQ-A1431182

Title: BUSINESS RECORDS ORDERS UNDER 50 U.S.C. § 1861

Synopsis: Provides guidance on the preparation, approval, and service of Business Record Orders, implementing 15 U.S.C. §1861 of the Foreign Intelligence Surveillance Act (FISA), as amended by the 2001 USA Patriot Act.

Reference: 66F-HQ-A1431182

Enclosure(s): Model Business Records Order Form and Instruction Sheet

Details: Public Law 107-56, the USA Patriot Act, contained several significant provisions with respect to expanding the scope of investigative techniques available in national security investigations. One of the provisions was the expansion of the scope of business records that may be obtained from an order issued by the FISA Court (FISC).

1. Introduction to Procuring Business Records

Prior to 1998, there was no provision in FISA nor any other statutory provision that authorized the FBI to obtain business records for a national security investigation other than the telephone, financial, and credit information available

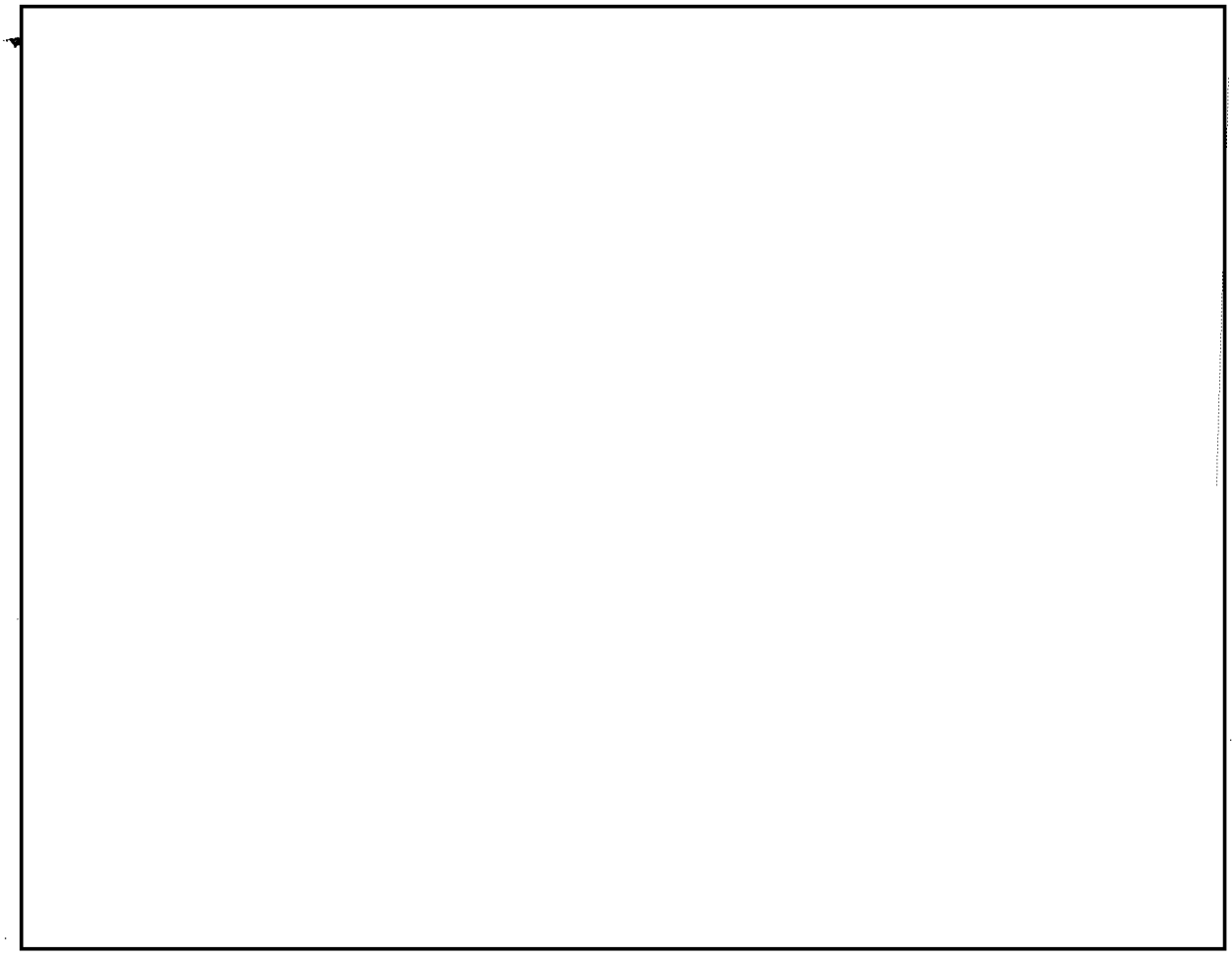
through national security letters. In 1998, FISA was amended to authorize an application to the FISC to procure certain limited types of business records, namely, those of a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility. Further, the amendment provided that the applicant must establish "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power," in addition to the requirement that the information is "sought for" a foreign intelligence or international terrorism investigation.

The 2001 Patriot Act expanded the scope of business records that are available pursuant to a FISC order. Currently, we can obtain "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person [USP] is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Further, the Patriot Act eliminated the requirement for a business record order that the person to whom the documents pertain is a foreign power or agent of a foreign power, just as it eliminated similar criteria for national security letters and pen registers. Thus, the requirements for a FISC business record order are very similar to those for a FISC pen register order. Basically, the records must be sought for an investigation authorized under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). Consistent with that requirement, the investigation must be to obtain foreign intelligence information not concerning a USP or to protect against international terrorism or clandestine intelligence activities. The investigation, if of a USP, cannot be solely based upon First Amendment activities.

The business records statute, 50 U.S.C. §1861, also provides that upon submission to the FISC of an application certifying that the request fits within the parameters of the statute, the FISC shall issue an ex parte order approving the release of the records if the court finds that the application meets the requirements of the statute. The ex parte order may not disclose that it was issued for purposes of an authorized investigation. Moreover, the person upon whom the order is served may not disclose to any other person, other than those persons necessary to produce the tangible things, that the FBI has sought or obtained the records.

[redacted] b1 b5 (S)

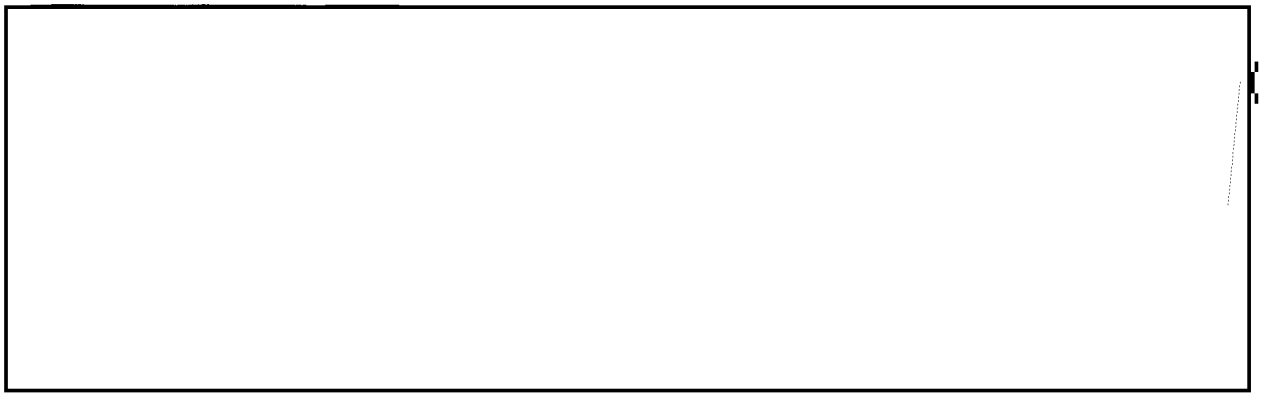
b1
b5



(S)

2)Process of Obtaining Business Records

The first step in the process of obtaining business records is to complete the Business Records Form, attached herein



(S)

b1
b5

to this EC. The form requests information required under the law as well as information needed for administrative purposes.

A. General Information

The form requires that the party requesting the business records identify the target [redacted] (S) b1 b5 for which the records are sought, the file number, and the date [redacted] (S)

Other administrative provisions relate to the identity of the field of origin, the case agent, and the headquarters SSA. Information is also requested concerning the status of the target of the investigation, and [redacted] (S) b1 b5

B. Basis of Request for Tangible Things

Thereafter, the form provides for the requesting party to give a description of the business records or other tangible objects that are sought, why the requesting party believes the records are in the possession of the custodian to whom the request is directed, and whether the originals of the records are sought or whether copies will suffice. Note that if you request copies, the order served upon the custodian will mandate that he/she maintain the originals of the records for two years unless notified by the FBI that earlier destruction is permissible.

In order to justify the request, the requesting party must then describe the investigation for which the business records are sought and the manner in which it is expected that the records will provide foreign intelligence information of value to the investigation.

C. Service of the Order

The requesting party must provide the name, address, title, and telephone number of the custodian of records upon whom to serve the order.

D. Field Office Approval

The Business Records Form must be approved by the SSA, CDC, and SAC (or program ASAC) at the field level.

E. Cover EC to Headquarters

The Business Record Form should be transmitted to headquarters via a cover EC to NSLB requesting that it prepare the application and proposed FISC order and present the package to the FISC. A copy of the Business Record Form should also be sent to the substantive headquarters unit and to the FISA unit.

3. NSLB Preparation of Application and Order

NSLB will review the business records request and, assuming it meets the requirements of the law, will prepare an application and proposed order[2] to be transmitted to the FISC. We expect that such an application and proposed order can be prepared within a few days of NSLB's receipt of the business records request form.

Approval authority for the application is housed at headquarters. On October 10, 2003, the authority to approve the application was delegated by the Director to the Deputy Director, the Executive Assistant Director for Counterterrorism/Counterintelligence, the Assistant Director and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions, the General Counsel, the Deputy General Counsel for National Security Affairs, and the Senior Counsel for National Security Affairs. It is expected that, unless availability becomes a problem, the application will be signed by attorneys within the General Counsel's office.[3]

[redacted] (S)

b1
b5

[3]Since this will mark the first time that the business record procedure has been used, it was determined that approval authority should remain at headquarters in the initial stages. Once a routine practice has been established and any problems or issues have been resolved, consideration will be given to delegating the approval authority to the field. However, the practical effects of such delegation may be minimal, inasmuch as

Once the application and proposed order have been prepared, they will be presented to the FISC by an attorney either from OGC or from OIPR. Unless there is reason to do otherwise, the application and proposed order will be presented at the FISC's regularly scheduled Friday hearings.

Upon signature by the FISC judge, a conformed copy of the order (a copy with an official marking by the FISC Clerk attesting that it is a true and correct copy of the original document) will be forwarded to the FISA Unit at headquarters. Thereafter, FISA Unit will email a copy of the conformed copy of the order to the appropriate field office for service and to the case agent (i.e., the point of contact on the order). The case agent and field office should receive the email within several days of the signing of the order.[4]

CONCLUSION

Any questions about the business records process should be addressed to Office of General Counsel, Assistant General Counsel [redacted], at [redacted]. b2 b6 b7C

---

the application must be made to the FISC and attorneys from OGC and/or OIPR, of necessity, will need to shepherd the paperwork through the process, regardless of who signs the application.

[4]We expect that the process currently used with regard to FISC orders will also apply in the future to business records orders. That is, per suggested Court procedures (although practice often differs), the FISA Unit should receive the conformed copy of FISC orders within a day or two of their signing. Once received by the FISA Unit, the Unit scans the orders and emails them to the appropriate office within 24 hours. While recipients of FISC orders to date generally have not required the original of the signed document, it is possible that the recipient of the business record order, likely an entity that never heard of the FISC, much less a FISC order, will require the original of the signed order. In that event, arrangements will need to be made with the FISA Unit to procure the original of the order. Further, if it is necessary for the office serving the business record order to receive the document sooner than set forth above, i.e., if there is a need for a "walkaway" copy, arrangements will need to be made with the Clerk of the FISC well ahead of the signing.

To: All Field Offices From: General Counsel
Re: 66F-HQ-A1431182, 10/29/2003

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to all supervisory personnel involved in the investigation of counterintelligence and counterterrorism cases.

(Revised 7/ 11, 2003)

FBI FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)
BUSINESS RECORDS REQUEST FORM

INSTRUCTIONS

The FBI must use this form to request that the National Security Law Branch (NSLB) prepare an application to the Foreign Intelligence Surveillance Court (FISC) for a Business Records Order, pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §1861.

FBI field offices must adhere to the following procedures in using this form:

(1) The FBI special agent (SA) in the relevant FBI field office/division with primary responsibility for the foreign counterintelligence or counterterrorism investigation to which the request relates should complete this form.

(2) This form must be reviewed and approved by Supervisory Special Agent (SSA), the Chief Division Counsel (CDC), and the Special Agent in Charge (SAC) or the Program Assistant Special Agent-in-Charge(ASAC).

(3) This form should be sent to the appropriate FBI Headquarters division (Counterintelligence or Counterterrorism), the National Security Law Branch (NSLB), Room 7975, and the FISA Unit, Room 1B046.

Based on the information provided on this form, NSLB will prepare a FISA Business Records Application, and Order and present it to the FISC.

Direct any questions about how to complete this form to the FBI HQ SSA or NSLB (202) 324-3951.

Blank versions of this form are unclassified. **Add classification markings to the form according to the classification of the information you provide.**

(Classification of completed form)

(Revised 7/11/03)

FISA REQUEST FOR ACCESS TO BUSINESS RECORDS, I.E., "ANY TANGIBLE THING (INCLUDING BOOKS, RECORDS, PAPERS, DOCUMENTS AND OTHER ITEMS)" (50 USC Section 1861)

1. **General Information**

   a. **Name of Subject(s) of the investigation for which the tangible things are sought:**

   b. **FBI file number(s):**

   c. **Date full investigation(s) of such subject was authorized:**
   [Note: If new FCI Guidelines are approved, it may allow for use of this technique in a preliminary investigation]

   d. **Office of origin:**

   e. **Case Agent Point of Contact:**
      i. **Name:**
      ii. **Telephone:**
      iii. **Secure Fax:**

   f. **FBI Headquarters SSA:**
      i. **Name:**
      ii. **Telephone:**
      iii. **Secure Fax:**

   g. **Status of Subject of the Investigation**
      i. **USP**
      ii. **Non-USP or**
      iii. **Foreign power**

   h. **Status of Subject of the Request, if different from Subject of the Investigation**
      i. **USP**
      ii. **Non-USP**
      iii. **Foreign Power**

2. **Basis of Request for Tangible Things**

   a. **Specifically describe the tangible things (e.g. books, records, papers, documents) you are requesting. If the tangible thing is not a written document (e.g., an apartment key), explain why you believe that it is being kept by a custodian in the**

normal course of business. Note that the subject of the request does not have to be the subject of the investigation.

b. If relevant, state whether you are requesting the original or copy of the tangible things.

c. Provide a brief summary of the full investigation for which the requested tangible things are sought [or summarize relevant preliminary investigation, if new FCI Guidelines so allow]

d. Explain the manner in which the requested tangible things are expected to provide foreign intelligence information for the full investigation [or preliminary investigation, if new FCI Guidelines so allow].

3. Service of the Business Records Order

a. Identify the current custodian, owner, or person in possession of the requested tangible things.

b. Identify the name, address, title, and telephone number of any custodian or person to whom an order needs to be directed to require the production of the requested tangible things.

4. Field Office Approval

I have reviewed this request and certify that the requested tangible things are sought for an authorized investigation, conducted in accordance with the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations, to obtain foreign intelligence not concerning a USPER or to protect against international terrorism or clandestine intelligence activities. I further certify that the authorized investigation is not being conducted solely upon the basis of activities protected by the First Amendment of the Constitution.

Supervisory Special Agent (SSA) approving this form:
Printed (or Typed) Name:
Telephone Number:

Signature: **Date:**

(Classification of completed form)

CDC approving this form:
Printed (or Typed) Name:
Telephone Number:

Signature: **Date:**

SAC or Program ASAC approving this form:
Printed (or Typed) Name:
Telephone Number:

Signature: **Date:**

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 3
Page 2 ~ Referral/Direct
Page 3 ~ Referral/Direct
Page 4 ~ Referral/Direct

Memorandum from [redacted] to General Counsel b6
Re: Response to OLP on Use of Patriot Act, 03/15/2004 b7C

Section 212 - Emergency Disclosure of Electronic Communications to Protect Life and Limb b1

b2
b7E

[redacted] (S)

- [redacted] b2 b7A b7E

[redacted] Due in part to the quick response allowed by Section 212, agents were able to quickly close this case with the suspects arrest. (See attached press release dated 7/11/03.)

- **Recent Kidnaping Case** - Recently, a 14 year old girl was abducted. Her laptop was also missing. The case agents suspected that the nefarious character she had met in an Internet chat room was the perpetrator [redacted] b7A

[redacted] e-mail. As a result, the suspect was quickly identified and interviewed. He admitted to picking up the girl and took agents to the truck stop where he had left her. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of

b6
b7C

(LE SENSITIVE) In this case it was difficult to identify the hacker because he [redacted] each time he entered the corporate victim's computer because he was [redacted] each time. Due to the changes in Section 216 of the USA PATRIOT Act, the FBI was able to obtain [redacted] for this hacker and then present it to [redacted] This enabled the agents to identify the hacker. He was recently arrested and is awaiting trial. (LE SENSITIVE)

b7A

Section 217 - Interception of Computer Trespasser Communications

- [redacted]

b2
b7A
b7E

- **(LE SENSITIVE) U.S. Government System Hacked** - Recently a U.S. Government computer system was identified as the victim of a computer hacker. The hacker was utilizing the government computer to [redacted] The investigation is ongoing to identify the suspect and any additional victims. (LE SENSITIVE)

b2
b7A
b7E

SUNSET PROVISIONS IN THE PATRIOT ACT

- Many of the investigative tools provided in the Patriot Act are governed by sunset provisions which will expire on December 31, 2005, unless renewed by Congress.

- There are approximately14 sunset provisions which apply mainly to tools that have enhanced our surveillance procedures (Title II of the Patriot Act). See attached chart, pages 1 - 4..

- The Office of the General Counsel (OGC), through the Chief Division Counsels, is encouraging field offices to keep records of the effective use of these tools and to provide this information to OGC so that the FBI will be prepared to justify their renewal.

CA# 05-CV-0845

PATRIOT ACT

TITLE NUMBER, SECTION NUMBER, (Statute amended or created)	Sunset Provision 12/31/05	Tracking	CITING DOCUMENT
Title II, Enhanced Surveillance Procedures, **Section 202**, Authority to Intercept Voice Communications in Computer Hacking Investigations (18 U.S.C. 1030)	yes		DOJ Guidance, p.1
Title II, Enhanced Surveillance Procedures, **Section 203(d)**, Authority to share criminal investigative information (50 U.S.C. § 401a)	yes		NSLU EC dtd 10/26/01 re: FISA, pg. 3
Title II, Enhanced Surveillance Procedures, **Section 206**, Roving surveillance authority under FISA (50 U.S.C. 1805(c)(2)(B))	yes		NSLU EC dtd 10/26/01 re:FISA, pg. 3
Title II, Enhanced Surveillance Procedures, **Section 207**, Duration of FISA Surv. of Non-US persons who are agents of a foreign power (50 U.S.C. 1805(e)(1))	yes		NSLU EC dtd 10/26/01 re: FISA, Pg. 4
Title II, Enhanced Surveillance Procedures, **Section 209**, Obtaining Voice-mail and Other Stored Voice Communications (18 U.S.C. 2703, 2510(1))	yes		DOJ Guidance, p.1
Title II, Enhanced Surveillance Procedures, **Section 210**, Scope of Subpoenas for Electronic Evidence (18 U.S.C. 2703(c)(2))	no		DOJ Guidance, p.2

Title II, Enhanced Surveillance Procedures, **Section 211**, Clarifying the Scope of the Cable Act (47 U.S.C. 551, 18 U.S.C. 2510, 18 U.S.C. 2701, and 18 U.S.C. 3121)	yes		DOJ Guidance, p.3
Title II, Enhanced Surveillance Procedures, **Section 212**, Emergency Disclosures by Communications Providers (18 U.S.C. 2702(b), 2703(c)(2)(F))	yes		DOJ Guidance, p. 4
Title II, Enhanced Surveillance Procedures, **Section 213,** Authority for Delaying Notice of the Execution of a Warrant (18 U.S.C. 3103a)	no		DOJ Guidance, p. 5
Title II, Enhanced Surveillance Procedures, **Section 214**, Pen Registers and Trap and Trace Authority Under FISA (50 U.S.C. 1842)	yes		NSLU EC dtd 10/26/01 re: FISA, pg. 4
Title II, Enhanced Surveillance Procedures, **Section 215**, Access to Records and Other Items Under the FISA (50 U.S.C. 1861)	yes		NSLU EC dtd 10/26/01 re: FISA, pg. 6
Title II, Enhanced Surveillance Procedures, **Section 216**, Pen Register and Trap and Trace Statute (18 U.S.C. 3121, 3123, 3124, and 3127)	no		DOJ Guidance, p. 6
Title II, Enhanced Surveillance Procedures, **Section 217**, Intercepting the Communications of Computer Trespassers (adds new section, 18 U.S.C. 2511, and amends 18 U.S.C. 2510))	yes		DOJ Guidance, p.9

Section	Includes Criminal and Terrorism Investigations	Terrorism and CI Investigations	Only Terrorism Investigations
203(a)		Information Sharing (Grand Jury)	
203(b)		Information Sharing (Title III)	
203(d)		Information Sharing (intelligence info obtained in the course of a criminal investigation)	
206		Roving FISA Authority	
207		Extended duration of FISA authority - also expanded FISC	
209	Voice mail - can be obtained with a search warrant		
210	Expanded subscriber information that can be obtained with a subpoena		
212	Voluntary disclosures by Internet Service Providers for emergencies		
213	Delayed notice for search warrants (sneak and peak warrants)		
214		FISA - change to pen/trap standard	
215		FISA - changed standard for business records authority	
216	Nationwide effect of pen/trap orders		
217	Computer trespasser		

	exception to the wiretap statute		
218		FISA - changes "primary purpose" standard to "significant purpose"	
219			Nationwide search warrants
220	Nationwide search warrants for e-mail		
223	OPR inquiry for improper disclosure of information pursuant to TIII, ECPA, pen/trap and trace, NSLs	Established civil liability for unauthorized disclosure of FISA information	
225		Grants immunity from civil liability for persons providing information in response to FISA order.	

~~SECRET~~

(Rev. 01-31-2003)

CA# 05-CV-0845

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/23/2004

To: All Field Offices **Attn:** SAC/ADIC
FBIHQ, Manuals Desk

All Legats **Attn:** Legat

Counterterrorism **Attn:** AD Gary Bald

Criminal Investigative **Attn:** AD Grant D. Ashley

Cyber **Attn:** AD Jana D. Monroe

Counterintelligence **Attn:** AD David W. Szady

From: Office of the General Counsel
Investigative Law Unit/Room 7326
Contact: [redacted] b2 b6 b7C

DATE: 12-13-2005
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-13-2030

Approved By: Caproni Valerie E
Curran John
Kelley Patrick W
[redacted] b6

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Drafted By: [redacted] b7C

Case ID #: 66F-HQ-C134260 (Pending)
66F-HQ-C1384970

Title: USA PATRIOT Act
Sunset Provisions

Synopsis: Many of the investigative tools created by the USA PATRIOT Act will sunset or expire on December 31, 2005 unless Congress acts otherwise. Details on the use of these tools are necessary to assist in justifying the continued need for these investigative tools. Offices are to provide the Investigative Law Unit, Office of the General Counsel (OGC) with statistics, good examples or anecdotes, or at the very least, a brief narrative summarizing the benefits the office has received from these provisions by March 9, 2004.

Reference: 66F-HQ-1085160- Serial 57

Details: The USA Patriot Act contained numerous provisions which are scheduled to sunset on December 31, 2005 unless Congress acts otherwise. The DOJ and the FBI are now beginning the process of demonstrating the continuing need for these investigative tools so that Congress will renew the viability of these tools. Specific cases where these provisions were of assistance will be instrumental in securing their renewal. For this reason, in June of 2002, when the OGC issued guidance on the provisions addressing investigative issues (see above referenced EC), it encouraged offices to keep records of the effective use of these tools. The EC also stated that

"important information to be maintained includes both the number of times the investigative tool was effectively used and specific information on noteworthy cases." This type of information will be critical in defending the need for these tools. If we do not take the time to set forth a strong defense complete with real examples of the effectiveness of these tools, Congress will likely let these investigative tools expire, thus reducing our arsenal against terrorism and other serious crimes.

In this regard, offices are requested to provide statistics, good examples and anecdotes, or at the very least, a brief narrative summarizing the benefits the office has received from these provisions. The information should be forwarded to the Investigative Law Unit, Office of the General Counsel (Room 7326) by March 9, 2004. Thereafter, offices are encouraged to continue providing the Investigative Law Unit new information on the use of these provisions as it becomes available. The following is a list of the sunset provisions and a brief description of the provision. Additional information is available on each provision as noted in the description below or in the above referenced EC.

Voice Mail - Section 209 of the Act enabled law enforcement to obtain all voice mail which is stored by a communications provider, [redacted] using the procedures set forth in 18 U.S.C. §2703 (such as a search warrant). This also applies to other wire communications as defined by the statute. [redacted] Previously the law was vague on the standard required to compel production of a stored voice mail message, leaving the possibility for argument that a wiretap order was required. See 18 U.S.C. § 2510; 18 U.S.C. § 2703. b2 b7E

Nationwide Search Warrants for E-mail and Associated Records - Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, [redacted] Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703. b2 b7E

Voluntary Disclosures - Section 212 of the law explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers. This provision also allows a communications service provider to disclose non-content records to protect their rights and property. This portion of the provision will most often be used when the communications service provider itself is a victim of computer hacking. See 18 U.S.C. § 2702(b) & (c)(3); 18 U.S.C. § 2703(c)(2)(F).

For about ten months (January 2003-November 2003) there was a mandatory reporting requirement for the receipt of content information (usually e-mail content) under this emergency disclosure provision. (See the Homeland Security Act and EC 66F-HQ-C1384970 Serial 501.) [redacted] b2 b7E

Information Sharing - Section 203(b) & (d) of the Act provided new information sharing capabilities between criminal and intelligence investigations for foreign intelligence information and information obtained via a Title III electronic surveillance. (See EC 66F-HQ-A1247863-71 dated 10/26/01 for additional information.) Recognizing that this tool has become a regular part of how the FBI operates, especially in terrorism cases, no statistics are necessary. However, any case examples that demonstrate the importance of this tool should be provided.

Intercepting Communications of Computer Trespassers - Section 217 of the Act clarified an ambiguity in the law by explicitly providing victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer. Additionally, based on the definition of a "computer trespasser," communications of users who have a contractual relationship with the computer owner may not be monitored, even if their use is in violation of their contract terms (i.e. spammers). See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

Expanded Predicates for Title III - Sections 201 & 202 of the Act expanded the predicate offenses for Title III to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). See 18 U.S.C. § 2516.

Roving FISA Surveillance - Section 206 amends FISA to allow the Court to issue [redacted] where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that [redacted]

(S) (S)

(S)

b1
b2
b5
b7E

[redacted] For additional information see EC 66F-HQ-A1247863-71 dated 10/26/01.

New Standard for FISA Pen/Trap - Section 214 of the Act eliminated the requirement that the FISA pen/trap order include specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. [redacted]

[redacted]

b2
b5
b7E

the basis of activities protected by the first amendment to the Constitution." For additional information see EC 66F-HQ-A1247863-71 dated 10/26/01.

New Standard for Business Records under FISA - Section 215 changed the business records authority found in Title V of FISA. The old language allowed the FISA Court to issue an order compelling the production of certain defined categories of business records (the records of common carriers, public accommodations, vehicle rentals, and storage facilities) upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. Section 215 changes this standard to simple relevance (just as in the FISA pen register standard described above) and gives the Court the authority to compel production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This is the same standard described above for Section 214. For additional information see EC 66F-HQ-A1247863-71 dated 10/26/01.

The Attorney General has stated that this provision has not be utilized, so no statistics are sought for this provision. However, any information is sought on cases where this provision would have provided significant assistance.

All submissions should be made via EC to the attention of [redacted] Investigative Law Unit, Office of the General Counsel, FBIHQ Room 7326 by March 9, 2004. Questions should be directed to either Assistant General Counse[redacted] or Unit Chief [redacted]

b2
b6
b7C

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Offices are to provide the Investigative Law Unit, Office of the General Counsel (OGC) with statistics, good examples or anecdotes, or at the very least, a brief narrative summarizing the benefits the office has received from these provisions by March 9, 2004.

CC: Ms. Caproni
Mr. Kelley
Mr. Curran
[redacted] b6 b7C
ILU - 2

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/11/2004

To: Records Management **Attn:** Manuals Desk,
Room 10471

From: Office of the General Counsel
Investigative Law Unit, Room 7326
Contact: [redacted]

Approved By: Kelley Patrick W [redacted] b6 b7C

Drafted By: [redacted]

Case ID #: 66F-HQ-A1085154-MISC (None)
66F-HQ-A1192083 (None)

Title: PROPOSED CHANGE IN THE MANUAL OF ADMINISTRATIVE OPERATIONS AND PROCEDURES, PART 2, SECTION 9

Synopsis: To update information contained in the MAOP, P2, Section 9. Upon approval of this communication, this EC should be forwarded to the Manuals Desk for handling.

Reference: 66F-HQ-C1185915 Serial 63

Details:

REASON FOR CHANGE

Changes to the MAOP, P2, Section 9, are necessary to update citations to laws, regulations, and guidelines, and to clarify existing language. Obsolete existing language is deleted by ~~strikeout~~ and new language is redlined. Instructions are in **bold** type.

CHANGED TEXT

SECTION 9. DISSEMINATION AND SHARING OF INFORMATION

Since the events of Tuesday, September 11, 2001, the Department of Justice has shifted its priorities to the protection of the American people and to enhancing the nation's security. This mission was fully stated in a Memorandum for Heads of Department Components dated November 8, 2001, and signed by Attorney General Ashcroft.

Because the prevention of terrorist activity is the overriding priority of the Department of Justice and improved

description of the facts and circumstances giving rise to the need for an exception and why lesser measures such as use restrictions are not adequate." Authority to request exceptions has not yet been delegated below the level of component agency head (and it is not clear whether it will be). For now, therefore, FBI requests for exceptions can only be submitted by the Director.

Any FBI requests for exceptions should be submitted for review and approval to CID and CTD. CID and/or CTD will then forward the requests to the Director's Office. OGC will be available to provide assistance with regard to any such requests.

Closed Investigations

OGC has concluded, in consultation with DOJ, that there is no legal impediment to sharing foreign intelligence information acquired in criminal investigations which have been closed. If there is reason to believe that a particular closed file(s) contains foreign intelligence information, the field office should conduct a review of the file(s).

Disclosure of Grand Jury and Title III Information

Where grand jury or Title III information is shared under the guidelines, notice of such disclosures must be promptly provided to DOJ's Office of Enforcement Operations (OEO). The guidelines require OEO to establish appropriate record keeping procedures to ensure compliance with notice requirements related to the disclosure of grand jury information. Agents do not have to contact OEO themselves; that is the obligation of the AUSA or DOJ prosecutor assigned to the grand jury matter or Title III.

Section 203 of the PATRIOT Act authorizes the sharing of foreign intelligence, counterintelligence, and foreign intelligence information obtained through grand jury proceedings and Title III interceptions with relevant Federal officials (i.e., any Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials) to assist in the performance of their duties. At the same time, section 203(c) requires the Attorney General to establish procedures for the disclosure of grand jury and Title III information that identifies United States persons. A "United States person" means a citizen of the U.S.; an alien lawfully admitted for permanent residence; an unincorporated association with a substantial number of U.S. citizens or lawfully admitted aliens for permanent residence; or a corporation which is

incorporated in the U.S. It does not include a corporation or an association which is a foreign power.

AGGs implement section 203(c) by establishing the required procedures for labeling grand jury and Title III information which identifies United States persons. Such information must be marked, prior to disclosure, to indicate that it contains such identifying information. Information should be marked if it identifies any United States person (i.e. the person need not be a target or a subject). However, the United States person must be "identified;" i.e., the grand jury or Title III information must discuss or refer to the U.S. person by name (or nickname or alias), rather than merely including potentially identifying information (e.g. an address or telephone number) which requires additional investigation to link to a particular person.

For the time being, no particular language or method of marking is required. The information must be clearly marked, however, in a manner which will ensure that the recipient will immediately understand that the information identifies United States persons. One way to do this, for example, would be to place the information in a sealed envelope marked with the following language in conspicuous lettering: "NOTE: THIS PACKAGE CONTAINS INFORMATION WHICH IDENTIFIES UNITED STATES PERSON(S)." Agents should also specifically direct the recipient to the references to identified U.S. persons.

Agents need not rely solely on the grand jury or Title III information itself in determining whether the information identifies a United States person; Agents may also use the context and circumstances of the information in making that determination. b5

The **Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources** implement section 905(b) of the PATRIOT Act, which requires the Attorney General to develop guidelines to ensure that DOJ responds within a reasonable period of time to reports from the intelligence community of possible criminal activity involving

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Friday, May 14, 2004 4:36 PM
To: [redacted] Div00) (FBI)
Subject: Patriot Act examples

b6
b7C

UNCLASSIFIED
NON-RECORD

b6 b7A
[redacted]
b7C

[redacted] is checking on the status of [redacted] If she does not reach me today, she will contact you on Monday morning with any information she obtains.

In reviewing my files, I do not have any outstanding examples to provide at this time. Listed below is one case number with all the information that the field office provided to me on this case. I offer it in the hopes that it might provide you a good case example.

b2
b7E

315C [redacted] 56983 - example sharing of intelligence information - a criminal case CW provided information regarding the subject of a foriegn intelligence investigation who was suspected of planning a terrorist act. Sharing of the intelligence information developed regarding the subject led to the interception, arrest and anticipated deportation of the subject.

I have also included my current draft summary of the results from my field survey on the use of the sunset provisions. As you will see, it is still clearly a draft document, but it might provide you some additional information.

Should you have any further questions, please feel free to contact me. I will be out of the office on Monday, but back on Tuesday morning.

Best wishes in your efforts.

[redacted]
Assistant General Counsel
Investigative Law Unit
Office of the General Counsel
[redacted]

b2
b6
b7C

UNCLASSIFIED

Sunset Provisions to Collect Cases of Interest for Renewal

INFORMATION SHARING
- foreign intel obtained in Title III and criminal investigations (§§ 203(b) & (d))

VOICE MAIL
-obtained under 18 USC §2703 (§ 209)

NATIONWIDE SEARCH WARRANTS FOR ELECTRONIC EVIDENCE

These provisions of the Patriot Act will sunset or expire on 12/31/2005. Justification of these provisions will likely be required to obtain their renewal. Specific cases where these provisions were of assistance will be instrumental in securing their renewal. Please forward such examples to the Investigative Law Unit, Office of the General Counsel.

Additional Sunset Provisions (Examples most likely to be collected by others)

NEW TITLE III PREDICATES
-§ 1030 and terrorism offenses (§§ 201 & 202)

ROVING FISA SURVEILLANCE
-(§ 206)

NEW STANDARD FOR FISA PEN/TRAP
-(§ 214)

NEW STANDARD FOR BUSINESS RECORDS UNDER FISA
-(§ 215)

CHANGES TO "PRIMARY PURPOSE" STANDARD IN FISA
-allows greater consultation with criminal investigators and prosecutors without putting FISAs at risk. (§ 218)

DISCLOSURE OF RECORDS BY COMPUTER HACKING VICTIMS
-(§ 212)

MONITORING COMMUNICATIONS OF COMPUTER TRESPASSERS
-victims of computer hacking may allow law enforcement to monitor trespassers on their computers (§ 217)

PERMITS CLAIMS AGAINST US FOR DISCLOSURE OF SENSITIVE INFORMATION
-(§ 223)

[redacted] (OGC) (FBI)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-03-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

From: [redacted]
Sent: Tuesday, February 17, 2004 10:09 AM
To: [redacted] b6
Cc: KELLEY, PATRICK W. b7C
Subject: FW: Sunset provisions

[redacted] Please prepare an EC to follow your earlier one on the the PA--this one needs to seek help for DOJ's fight to retain the sunseting provisions. They want any or all of the following: stats (if they have them), good examples/antecdotes, and, if nothing else, at least a narrative summary of the beneifits the FO has seen in the provision. Just list the provisions that sunset, remind folks we suggested up front that they track this information and make it for the GC's signature and set 2 weeks as the deadline. Thanks

[redacted] b6
b7C

-----Original Message-----
From: Caproni, Valerie E.
Sent: Friday, February 13, 2004 1:13 PM b6
To: [redacted]
Subject: RE: Sunset provisions b7C

Sorry: I do recall this. There is nothing attached. Let's send an EC out as you request. Tasking can come from me.

I assume the personnel issue is your agent who is looking for different pastures?

-----Original Message----- b6
From: [redacted]
Sent: Friday, February 13, 2004 12:49 PM b7C
To: Caproni, Valerie E.
Subject: FW: Sunset provisions

Here is what I sent you on these sunset provisions

-----Original Message----- b6
From: [redacted]
Sent: Wednesday, February 11, 2004 4:50 PM b7C
To: Caproni, Valerie E.
Cc: [redacted]
Subject: Sunset provisions

[redacted] had a good thought about how to get what OLP wants to prepare for the "sunset." Attached is a draft of an EC that we sent out in June 2002 about the Patriot Act to all Fos. In it, we say that several provisions would sunset unless renewed and for that reason offices were "encouraged" to keep records of their use of these provisions. In addition, CDCs were advised to do that at the CDC Conference and given a handout of what provisions would sunset and again asked them to keep examples of their usefulness and to send them to ILU. We haven't received any.

[redacted]

In addition, DOJ (OEO) should have stats on the 203/905 dissemination of FGJ and T-3 info to the IC and we could refer OLP to them. Also, we do have some stats about § 212 (voluntary emergency disclosure of e-mail content by an ISP) in my office. Perhaps, as well, OLP could be directed to OIPR for some of the FISA sunset provisions--214 (pen/trap trace), 206 (roving FISAs).

b5

By the way, I need to discuss personnel issue with you when you have a moment.

[redacted] b6
b7C

PATRIOT ACT REPORTING REQUIREMENTS

TAB	PATRIOT SECTION AND THE REPORTING REQUIREMENTS
A	Requirement: Sec. 203 amends Fed. R. Crim. P. 6(e)(3)(C). New Rule 6(e)(3)(C)(iii) requires that within a reasonable time after disclosure, an attorney for the government "file under seal a notice with the court stating the fact that 6(e) information was disclosed and the departments, agencies, or entities to which the disclosure was made." [redacted] b5
B	Requirement: Sec. 205(c)(1) requires the FBI to report to the Department the number of translators employed by the FBI; any legal or practical impediments to using translators employed by other Federal, State, or local government agencies; the need for specific translation services in certain languages, and the FBI's recommendation(s) for meeting those needs. No date specified. [redacted] b5
C	Requirement: Sec. 215 amends 50 U.S.C. 1861 by adding sections 501 - 503. The new section (Section 502) requires the AG to submit reports on a semi-annual basis to Congressional Committees the total number of applications made, and the number of orders granted, modified, or denied under section 402 of the Foreign Intelligence Surveillance Act. [redacted] b5
D	Requirements: Sec. 403(b) states that the FBI shall provide access to NCIC to the State Dept. and INS via extracts, and give periodic NCIC extract updates. During the next 2 years, the AG shall report to Congress on the implementation of the amendments. The FBI will be required to give input for this report. [redacted] b5 b6 b7C

[redacted] (OGC) (FBI)

From: [redacted]
Sent: Friday, February 20, 2004 2:21 PM
To: [redacted]
Subject: Sunset Provisions

b6
b7C

I double checked (and triple checked) - Section 218 (change to the primary purpose standard) is a sunset provision. . . So unless Congress has acted otherwise already, or unless Congress acts, it will expire on 12/31/2005.

I confirmed all other sunset provisions I listed. There are two additional sunset provisions I did not address. 1 - (Section 204) assures that foreign intelligence gathering authorities are not disrupted by changes to the pen/trap statute. 2 - (Section 207) extends the initial authorization periods for certain FISA surveillance and search capabilities. I didn't see a need to address these originally, but can if you think otherwise.

[redacted]

b6
b7C

[redacted](OGC) (FBI) b6 b7C

From: [redacted](Div09) (FBI)

Sent: Friday, March 12, 2004 4:13 PM

To: [redacted] BOWMAN, MARION E. (Div09) (FBI) [redacted]

Cc: CHANDLER, CASSANDRA M. (Div00) (FBI)

Subject: Sunset Provisions of the PATRIOT Act

b6
b7C

UNCLASSIFIED
NON-RECORD

I thought you folks might be interested in the CRS report re the Sunset Provisions of the PATRIOT Act.

UNCLASSIFIED

~~SECRET~~

[redacted](OGC) (FBI) CA# 05-CV-0845

From: [redacted]
Sent: Friday, March 12, 2004 6:08 PM
To: [redacted](Div09) (FBI)
Subject: Fwd: Re 2001 USA Patriot Act

b6
b7C


10-18-2002 EC Assistance to SN...

10-16-2002 FD-302 Investigatio...

10-16-02 2702bc To Roar ng For...

10-15-02 2702c To Qwest for IP...

10-15-02 2702c To Rocky Mounta...

10-15-02 2702c To hotmail for ...

[redacted] I hope this helps!

b2
b6
b7C

[redacted]
Squad CR-18/NVRA
[redacted]

-----Original Message-----
Date: 03/12/2004 11:55 am -0500 (Friday)
From [redacted]
To:
Subject: Re 2001 USA Patriot Act

b6
b7C

[redacted]

b2
b7A
b7E

Re 2001 USA Patriot Act and sunset provisions:

1) I used the 18, USC, Sect. 2702(b) and (c) provisions of the 2001 USA Patriot Act during the [redacted] investigation in 2002 [redacted] Attached are copies of the EC documenting the use, FD-302, and letters to ISPs requesting information.
2) I believe [redacted] now an SSA w/ STAS and formerly of CR-16, used the same provisions [redacted] in 2002/2003. (S)
3) I believe WFO Squad IT-7 or whoever case number 265A-[redacted]-225876 is/was assigned to used the same provisions extensively in 2003.
4) SSA [redacted] had conducted campaigns at WFO for the usage of the sunset provivions of the PATRIOT act [redacted] since 2002 and would be a good POC for this matter. (S)

[redacted]

b1
b2
b6
b7C
b7E

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/18/2002

To: Washington Field b2

From: Washington Field b6
Squad CR-18 / NVRA
Contact: SA [redacted] b7C

Approved By: [redacted]

Drafted By: [redacted] pmdv

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-03-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

Case ID #: 66-WF-C220745 SUB F300 (Pending)
66-WF-C220745 SUB L30 (Pending) b2

Title: FIELD OFFICE - [redacted] b7E
LEGAL MATTERS - GENERAL

Synopsis: To document for files assistance provided to [redacted] in support of the [redacted] Case ID [redacted] and to document usage of the 18 U.S.C. 2702(b) and (c) provisions of the 2001 USA Patriot Act which are scheduled to be sunset.

Administrative: Reference Rapid Start Number [redacted] Case ID [redacted] b2

Enclosure(s): For each file, one copy of FD-302 dated 10/16/2002. b7A b7E

Details: The purpose of this EC is to document for file assistance provided by WF Squad CR-18 to [redacted] regarding Rapid Start Lead Number [redacted] Case [redacted] and to document for file usage of the provisions of the 2001 USA Patriot Act which are scheduled to be sunset.

See attached FD-302 for details.

♦♦

[redacted] (OGC) (FBI)

From: [redacted] Div09) (FBI) b6

Sent: Monday, March 15, 2004 11:21 AM b7C

To: Caproni, Valerie E. (Div09) (FBI)

Cc: KELLEY, PATRICK W. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (OGA)

Subject: OLP Request

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b5

Valerie: Attached is a memo containing what I could gather together on short notice to answer OLP's request for Patriot Act provision examples, etc. Most of the FISA related ones really have to come from CTD, NLSB, OIPR--and many of those [redacted] as I understand it--e.g., Sections 206 (roving FISA); 214 (FISA pens); 215 (FISA court order to produce records). When we get some response to the sunsent EC, I'll forward those.

[redacted] b2
Office of the General Counsel b6
[redacted] b7C

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted]
Sent: Friday, March 19, 2004 11:07 AM
To: [redacted] (Div09) (FBI)
Subject: Sunset provisions, Use of

b6
b7C

079ETC01.WPD (15 KB)

[redacted] I've reached out to all of our squad supervisors to confirm instances where these provisions have been used. There's not much but they are included in the attachment. I hope this helps. The electronic and hard copies will follow.

[redacted] (OGC) (FBI)

From: [redacted] (ME) (FBI) b6
Sent: Friday, March 19, 2004 12:57 PM b7C
To: [redacted] (Div09) (FBI) CA# 05-CV-0845
Subject: USA PATRIOT ACT SUNSET PROVISIONS

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-03-2005 BY 65179 DMH/CLS

[redacted] ttached to this communication is the Memphis field office response EC providing a narrative summary of use by the Memphis office. We have just switched to Trilogy and are having some problems uploading. Since this is the Buded, I am sending the EC to you as an attachment. I am hopeful that we will be able to successfully upload today so this will go into ACS now or as soon as possible. Call me if you have any questions at [redacted] [redacted] 66F-HQ-C

b2
b6
b7C

UNCLASSIFIED

[redacted]OGC) (FBI) b6

b7C

From: [redacted]
Sent: Friday, March 19, 2004 6:58 PM
To: [redacted]Div09) (FBI)
Subject: USA Patriot Act Sunset Provisions

b6

[redacted] b7C

Please note that I am still waiting to hear from a couple supervisors regarding the OGC inquiries set forth in the 2/27/04 EC. I know the deadline was 3/19/04, but if you could give me a couple more days it would be appreciated.

Thanks,

[redacted] b6

Acting CDC - Cleveland Division b7C

[redacted] (OGC) (FBI)

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-03-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

From: Caproni, Valerie E. (Div09) (FBI)
Sent: Tuesday, March 23, 2004 11:59 AM
To: [redacted] (Div09) (FBI)
Cc: [redacted] Div09) (FBI)
Subject: RE: Sunset provisions

UNCLASSIFIED
NON-RECORD

sounds good

-----Original Message-----
From [redacted] (Div09) (FBI)
Sent: Tuesday, March 23, 2004 11:48 AM
To: Caproni, Valerie E. (Div09) (FBI)
Cc: [redacted] (Div09) (FBI)
Subject: Sunset provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

Valerie: We are starting to get responses to our Sunset provisions EC that OLP asked you to collect. Although the other imminent requirement to collect all Patriot Act info for congressional testimony preparattion kind of took over, I assume the sunset collection requirement is still out there and will heat up more in time.

So, I told [redacted] to collect for about two more weeks and then put it together for your signature to send to OLP. Okay?

b2
b6
b7C

[redacted]
[redacted]
Office of the General Counsel
[redacted]

UNCLASSIFIED

UNCLASSIFIED

CA# 05-CV-0845

[redacted] The following is provided in response to your request for input on the sunset provisions of the PATRIOT Act. The three sunset provisions that the Baltimore Division has utilized and benefitted from the most are the information sharing, changes to primary purpose standard for FISA, and the nationwide search warrants. b6 b7C

[redacted] (S)

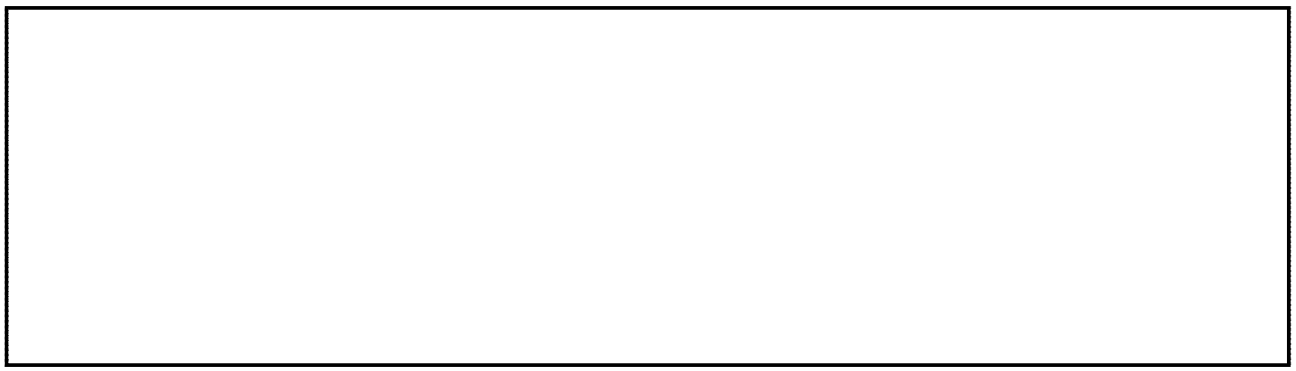
b1
b2
b5
b7E

[redacted] (S)

b1
b2
b5
b7D

Regarding the other sunset provisions of the PATRIOT Act, while we have not had many specific instances of implementing their use, it is certainly foreseeable that the need for their use could come up [redacted]

[redacted] b5



b5

[redacted] (OGC) (FBI)

CA# 05-CV-0845

From: [redacted] (Div09) (FBI) b6 b7C
Sent: Friday, April 30, 2004 12:50 PM
To: [redacted] (Div09) (FBI)
Subject: RE: Sunset Provisions - Section 207 - Extended FISAs for non-US persons

UNCLASSIFIED
NON-RECORD

I'll forward this to the units and get any info we have. Thanks.

-----Original Message-----
From: [redacted] (Div09) (FBI) b6 b7C
Sent: Friday, April 30, 2004 12:45 PM
To: [redacted] (Div09) (FBI)
Subject: Sunset Provisions - Section 207 - Extended FISAs for non-US persons

UNCLASSIFIED
NON-RECORD

[redacted] Somehow I missed section 207 when I sent out the EC seeking input from the field on the sunset provisions. This provision amended the time lines for FISA orders for agents of a foreign power. (extending the initial ELSUR orders to 120 days with 1 year renewals, and various timelines for physical searches depending on the target). [redacted] b5

[redacted] b6

thanks in advance for your help. b7C

[redacted]

UNCLASSIFIED

UNCLASSIFIED

DATE: 10-26-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 10-26-2030

CA# 05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] (OGC) (FBI)

From: [redacted] (CI) (FBI)
Sent: Monday, May 03, 2004 1:20 PM
To: [redacted] (Div09) (FBI)
Subject: RE: Sunset Provisions - Roving FISA order

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] (S)

-----Original Message-----
From [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:07 PM
To [redacted] (CI) (FBI)
Subject: FW: Sunset Provisions - Roving FISA order

b7C
b7D
b1
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

-----Original Message-----
From [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:03 PM
To [redacted] CI) (FBI)
Subject: Sunset Provisions - Roving FISA order

b6
b7C
b2
b6
b7A
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] Thanks for your response to our call to the field for examples using the sunset provisions. I'm compiling the results for the GC. In your EC, you noted that the [redacted] Can I get more info on this use? It seems like a good case to include as an example. Also let me know how you want it classified. You noted it was still an ongoing case, so should we classify it? or just label it law enforcement sensitive?

Thanks.

[redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

~~SECRET~~

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI) b6 b7C

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 11, 2004 12:00 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div09) (FBI) [redacted] Div09) (FBI) [redacted] (Div09) (FBI)
Subject: RE: Patriot Act Section 215 - after sunset

UNCLASSIFIED
NON-RECORD

b5

[redacted]

-----Original Message-----
From: [redacted] (Div09) (FBI) b6
Sent: Friday, May 07, 2004 6:05 PM
To: [redacted] (Div09) (FBI) b7C
Subject: FW: Patriot Act Section 215 - after sunset

UNCLASSIFIED
NON-RECORD

FYI
-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 04, 2004 4:54 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI) [redacted] (Div09) (FBI)
Cc: [redacted] (Div09) (FBI) b6
Subject: Patriot Act Section 215 - after sunset b7C

UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

In compiling the information received from our recent field survey on the various sunset provisions, I'm also reading a report recently prepared by the Congressional Research Service for Congress on the various sunset provisions. The report states that if Section 215 is left to sunset, "the impact of expiration may be mitigated by changes in the law governing 'national security letters' that provide access to a wider range of business records"

[redacted]

If you have any questions, please feel free to contact me. b5

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI) b6 b7C CA# 05-CV-0845

From: [redacted](Div09) (FBI)
Sent: Tuesday, May 11, 2004 1:11 PM
To: [redacted](Div09) (FBI); [redacted]Div09) (FBI)
Subject: RE: Patriot Act Section 215 - after sunset

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] The Report is titled "USA Patriot Act Sunset: Provisions that Expire on December 31, 2005" dated 1/2/04, written by Charles Doyle, Senior Specialist, American Law Division, of the Congressional Research Service. CRS Report RS21704. The quote I mentioned was on page CRS-9. I don't have a digital copy, but if you want a copy of my paper version, just let me know. --[redacted]

b6
b7C

-----Original Message-----
From: [redacted](Div09) (FBI)
Sent: Tuesday, May 11, 2004 12:00 PM
To: [redacted](Div09) (FBI); [redacted](Div09) (FBI)
Cc: [redacted]Div09) (FBI); [redacted]Div09) (FBI); [redacted](Div09) (FBI)
Subject: RE: Patriot Act Section 215 - after sunset

UNCLASSIFIED
NON-RECORD

[redacted] b5

-----Original Message-----
From: [redacted](Div09) (FBI)
Sent: Friday, May 07, 2004 6:05 PM
To: [redacted](Div09) (FBI)
Subject: FW: Patriot Act Section 215 - after sunset

b6
b7C

UNCLASSIFIED
NON-RECORD

FYI
-----Original Message-----
From: [redacted](Div09) (FBI)
Sent: Tuesday, May 04, 2004 4:54 PM
To: [redacted](Div09) (FBI); [redacted](Div09) (FBI); [redacted](Div09) (FBI)
Cc: [redacted](Div09) (FBI)
Subject: Patriot Act Section 215 - after sunset

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

In compiling the information received from our recent field survey on the various sunset provisions, I'm also reading a report recently prepared by the Congressional Research Service for Congress on the various sunset provisions. The report states that if Section 215 is left to sunset, "the impact of expiration may be mitigated by changes in the law governing 'national security letters' that provide access to a wider range of business records"

This seems to be a confident statement that we will not be impacted by the expiration of Section 215. I know that I have already found an error in the report regarding Title III issues, and have alerted OEO to the misstatement so that it can be corrected. I bring this to your attention to provide you the same opportunity should you disagree with the statement.

If you have any questions, please feel free to contact me.

[redacted]

b2

b6

b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Friday, May 14, 2004 9:55 AM
To: [redacted] Div00) (FBI)
Subject: FW: Sunset Provisions - Roving FISA
Importance: High

CA# 05-CV-0845

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I just received this from the field. See below and do NOT include this example in the Director's testimony. Sorry for this late notice.

b6
b7C

Could you also allow me the chance to review the draft before it is made final? Thanks.

I hope your writing is going well.

[redacted]

-----Original Message-----
From: [redacted] (KX) (FBI)
Sent: Wednesday, May 12, 2004 11:12 PM
To: [redacted] (Div09) (FBI)
Subject: RE: Sunset Provisions - Roving FISA

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-04-2005
CLASSIFIED BY 65179DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Sorry I took a while to get back to you. I asked the FCI Supervisor here about this very issue before sending the EC, and he advised at that time that he had no problem with sending the response as drafted to FBIHQ unclas with the information I placed therein. His opinion as I recall was based almost exclusively on the lack of specificity regarding the case a[redacted]

b1

(S) [redacted] and the work of the FBI and DOE Counterintelligence is well known there--in a general sense.

[redacted]

Thanks,

[redacted]
[redacted] Knoxville
[redacted]

b2
b6
b7C
b5

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:15 PM
To: [redacted] (KX) (FBI)
Subject: Sunset Provisions - Roving FISA

~~SECRET~~

~~SECRET~~

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] Thanks for your submission earlier. I am in the process of compiling the information for the General Counsel. I plan to include the following example from your EC, however, I noted that this was not considered classified in your EC. Do you want to protect it as classified or law enforcement sensitive? If not, it may end up being used publicly (i.e. in a Congressional hearing) as is.

[redacted] (S)

Thanks for your help.

b1
b2
b6
b7C

[redacted]
Assistant General Counsel
Investigative Law Unit
Office of the General Counsel
[redacted]

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

~~SECRET~~

[redacted] OGC) (FBI)

CA# 05-CV-0845

From: [redacted] (Div09) (FBI) b6
Sent: Friday, May 14, 2004 10:28 AM b7C
To: [redacted] (KX) (FBI)
Subject: RE: Sunset Provisions - Roving FISA

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] Thanks for this information. I'll make sure that this example does not end up in any public examples. Thanks again for your effort to compile this.

[redacted] b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-04-2005
CLASSIFIED BY 65179DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

-----Original Message-----
From: [redacted] (KX) (FBI)
Sent: Wednesday, May 12, 2004 11:12 PM
To: [redacted] (Div09) (FBI)
Subject: RE: Sunset Provisions - Roving FISA

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Sorry I took a while to get back to you. I asked the FCI Supervisor here about this very issue before sending the EC, and he advised at that time that he had no problem with sending the response as drafted to FBIHQ unclas with the information I placed therein. His opinion as I recall was based almost exclusively on the lack of specificity regarding the case [redacted] b1

(S) [redacted] and the work of the FBI and DOE counterintelligence is well known there--in a general sense.

Personally, I would NOT be comfortable having the paragraph you quoted published in a Congressional record, read aloud on C-SPAN, or otherwise addressed in a public forum, as it would have a chilling effect on other work we do out there using similar modus operandi. I am forwarding this message to him and will get back to you shortly.

Thanks, b2

[redacted] b6
Knoxville
[redacted] b7C

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:15 PM
To: [redacted] (KX) (FBI)
Subject: Sunset Provisions - Roving FISA

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

~~SECRET~~

[redacted] Thanks for your submission earlier. I am in the process of compiling the information for the General Counsel. I plan to include the following example from your EC, however, I noted that this was not considered classified in your EC. Do you want to protect it as classified or law enforcement sensitive? If not, it may end up being used publicly (i.e. in a Congressional hearing) as is.

[redacted] (S)

Thanks for your help.

[redacted] b1

Assistant General Counsel b2
Investigative Law Unit
Office of the General Counsel b6
[redacted] b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

[redacted] (OGC) (FBI)

CA# 05-CV-0845

From: [redacted] (Div09) (FBI)
Sent: Friday, May 14, 2004 10:30 AM
To: [redacted] (Div09) (FBI)
Cc: [redacted] (Div09) (FBI)
Subject: FW: Sunset Provisions - Roving FISA

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I just received this from the field. They no longer want one of the roving FISA examples to be used in any public testimony. (This example was in the draft that I had provided to you on Tuesday.) My apologies, however, if I recall you were most interested in the information sharing provisions instead.

Thank you,

b2
b6
b7C

[redacted]

-----Original Message-----
From [redacted] (KX) (FBI)
Sent: Wednesday, May 12, 2004 11:12 PM
To: [redacted] (Div09) (FBI)
Subject: RE: Sunset Provisions - Roving FISA

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Sorry I took a while to get back to you. I asked the FCI Supervisor here about this very issue before sending the EC, and he advised at that time that he had no problem with sending the response as drafted to FBIHQ unclas with the information I placed therein. His opinion as I recall was based almost exclusively on the lack of specificity regarding the case [redacted] and the work of the FBI and DOE Counterintelligence is well known there-- in a general sense. b1

(S)

Personally, I would NOT be comfortable having the paragraph you quoted published in a Congressional record, read aloud on C-SPAN, or otherwise addressed in a public forum, as it would have a chilling effect on other work we do out there using similar modus operandi. I am forwarding this message to him and will get back to you shortly.

Thanks,

b2
b6
b7C

[redacted]
[redacted] Knoxville
[redacted]

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 12:15 PM
To: [redacted] (KX) (FBI)
Subject: Sunset Provisions - Roving FISA

~~SECRET~~

b6

b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] Thanks for your submission earlier. I am in the process of compiling the information for the General Counsel. I plan to include the following example from your EC, however, I noted that this was not considered classified in your EC. Do you want to protect it as classified or law enforcement sensitive? If not, it may end up being used publicly (i.e. in a Congressional hearing) as is.

[redacted] (S)

Thanks for your help.

[redacted]

b1

Assistant General Counsel
Investigative Law Unit
Office of the General Counsel

b2

b6

[redacted]

b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

[redacted](OGC) (FBI) b6

From: [redacted](Div09) (FBI) b7C
Sent: Friday, May 14, 2004 12:53 PM
To: [redacted]Div00)) (FBI); [redacted](Div00) (FBI); [redacted](Div00) (FBI)
Cc: [redacted](Div00) (FBI); [redacted](Div00) (FBI); [redacted]Div09) (FBI)
Subject: RE: Draft Senate Judiciary Testimony for Director on 5/20/04

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Upon reviewing the portion of the attached document regarding the USA Patriot Act, I offer the following comments to ensure that it is legally accurate.

1) On page 2-3, the following text appears . . .

"For instance, if a court-ordered criminal wiretap turned up intelligence information, the criminal investigator could not share that national security information with the intelligence investigator – [redacted]

[redacted] b5

2) On page 5, the following text appears . . .

"Today, pen registers and trap-and-trace devices can be sought from a court for Internet communications."

Pen/trap orders were obtained for Internet communications prior to the Patriot Act, however, the Patriot Act did clarify the law to ensure that no judge could interpret the law otherwise.

Should you have any other additional questions regarding the Patriot Act, please feel free to contact me.

[redacted] b2
Assistant General Counsel
Investigative Law Unit b6
Office of the General Counsel
[redacted] b7C

-----Original Message-----
From: [redacted]Div00) (FBI)
Sent: Friday, May 14, 2004 10:09 AM
To: [redacted](Div00) (FBI); [redacted]Div00) (FBI)
Cc: [redacted](Div00) (FBI); [redacted]Div09) (FBI); [redacted]Div00) (FBI)
Subject: Draft Senate Judiciary Testimony for Director on 5/20/04

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Good morning [redacted]

Attached is a draft of the Senate Judiciary testimony, per your request. It covers the three main topics we covered in our discussion earlier this week -- the importance of the Patriot Act in the war on terror, counterterrorism and intelligence program reforms and improvements, and the current status of the FBI's IT/Trilogy.

Since we didn't talk in too much detail about what the FBI wants to say regarding IT, that section of the draft is fairly general, mentioning some important achievements and assuring that we continue to seek outside help to ensure we have the best products possible. Since I'm not too familiar with the in-the-weeds details of the current Trilogy problems that the Committee might address, you might want to run that part past [redacted] office to make sure it's in keeping with the FBI's message. b6 b7C

b6
b7C

Also, I am copying [redacted] in OGC -- she helped me to gather (and translate into English!) the Patriot Act details. She has offered to give it a read to make sure that section is accurate and ok to say in public.

[redacted] - I left the "DOCOEE" acronym highlighted for the moment until we get the translation we talked about yesterday. :)

b6
b7C

Hope this is helpful! Have a great Friday.

Thanks,

[redacted]
Executive Writing Unit
Office of Public Affairs
[redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

USA Patriot Act
Sunset Provisions
Field Office Comments
April 2004

Section 201 & 202 - Expanded Title III predicates

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing). Due to the timing and statutory placement of these two additional predicate offenses, it is likely that these are now included in the sunset provision.[1]

Survey Results: The respondents to the field survey indicated that there was at least one Title III order where terrorism was identified as the predicate offense.

Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. The Homeland Security Act later authorized disclosure to foreign investigative or intelligence officials and to any federal, state, local, and foreign official when it reveals a threat of attack.

Note: The Congressional Research Services (CRS) report to Congress on the sunset provisions erroneously states that "termination of authority under subsection 203(b) may be a little consequence."[2] In fact, the termination of this provision would have absurd results. [redacted] Essentially, [redacted] b5

Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. The Homeland Security Act also added foreign intelligence and investigative officials to the list of receiving officials. Due to the

[1]See CRS Report for Congress, "USA Patriot Act Sunset: Provisions That Expire on December 31, 2005," dated January 2, 2004., CRS Report RS 21704.

[2]CRS Report RS 21704 at 5.

placement of the Homeland Security Act amendments, the CRS concludes that these disclosure provisions will also terminate if 203(d) is allowed to sunset.

Survey Results: The information sharing provisions are systemically heralded as the most important provisions in the Patriot Act.

b2
b7E

-helps to prevent the compromise of foreign intell investigations
-the ability to share information has enhanced FBI liaison with State, Local and other Federal agencies, resulting in better relationships.
-Enables case agents to involve other agencies in investigations resulting in a style of teamwork that enables more effective and responsive investigations.
-improves the utilization of resources allowing a better focus on the case
-some field offices - White Collar Crime squads often generate leads that lead to IT investigations. Because the impediments to information sharing from the criminal side to the intelligence side have come down, these squads are now free to do so without hesitation. Even some limitations in information sharing would cause an agent to hesitate before sharing the information with his counterparts in the intelligence community. (?)
-Even Legats notice improved relationships with intelligence agencies.

Note - this is part of the information sharing provisions. The combination of all the information sharing provisions and the final FISA court decision resulted in the "wall" coming down. Since the entire "wall" has come down, all investigators are free to share information without hesitation. This has overall lead to a much more efficient and effective team approach to investigations. Overwhelmingly, the field sees this as the most important benefit of the Patriot Act. Some state that it would be virtually impossible to track and fight terrorists if the "wall" were still in place. Even if only parts of the "wall" are reinstated, then it will create hesitation on the part of agents before they share information leading to less teamwork, and much less efficiency.

b1
b2
b5
b7E

-Example - A criminal informant provided the FBI information that the subject of a foreign intelligence investigation was suspected of planning a terrorist act. The sharing of intelligence information led to the interception, arrest and anticipated deportation of the subject.

Section 206 - Roving FISA Surveillance

When a FISA target's actions have the effect of thwarting surveillance, [redacted] the Court can issue an order directing [redacted] etc., to effect the authorized electronic surveillance. [redacted] (S)

[redacted] (S)

b1

b1

[redacted] (S)

Section 207 - Extended Duration for Certain FISAs

Section 207 extends the standard duration for several categories of FISA orders.

[awaiting input from NSLB [redacted] on this] b6 b7C

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail.

b1

[redacted] (S)

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury. The Homeland Security Act modified this provision as it relates to the content of communications, but not as it relates to the records held by a service provider. For this reason, the Congressional Research Service concludes that only those provisions relating to the voluntary disclosure of records is subject to the sunset provision.[3]

[was 2702 (c)(3) part of this provision? - allows for voluntary disclosure of records to protect their own property and rights.]

[redacted] (S)

b1

[3]See CRS Report, page CRS-8.

b1

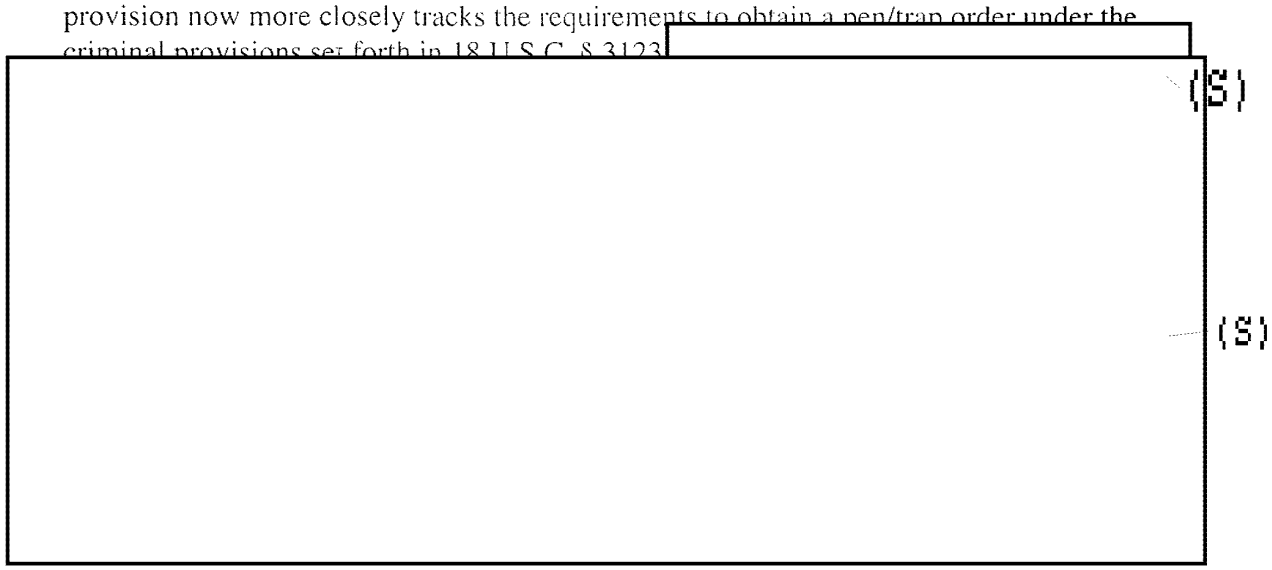
(S)

b7A

Section 214 - FISA Pen/Trap Authority

FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123.

b1



(S)

(S)

b1

[redacted] (S)

[redacted] (S)

Section 215 - Access to Business Records under FISA

b1

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records [redacted] to include "any tangible things (including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

b2

b7E

[redacted] (S)

-Again the field offices consistently report their frustration with the length of time to get any approvals from OIPR to utilize these provisions.

b1

One field office (Salt Lake?) confused the 215 stating it was an NSL. Check with them to determine which it was. (These are different provisions).

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI) b6
Sent: Tuesday, May 18, 2004 2:08 PM b7C
To: [redacted] (Div09) (FBI)
Cc: [redacted] Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

CA# 05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] we have not used 215, so if an office said they did, it meant that they submitted a request to me, but so far no luck on getting this presented to the FISC [redacted]

-----Original Message-----
From: [redacted] (Div09) (FBI) b6
Sent: Tuesday, May 18, 2004 2:03 PM b7C
To: [redacted] (Div00) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: Beers, [redacted] (Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] I can provide you the results from the field survey that OGC conducted, however, I can also guarantee that these are not entirely accurate numbers. The field survey was voluntary, and the level of detail provided varied between the field offices. Furthermore, since then I have been advised that some HQ divisions have been utilizing various Patriot Act tools, and I did not receive any contributions from any HQ division on this survey, so their use is not included in any numbers that I have.

The field offices reported the following: b1

Section 206 - Roving FISA orders [redacted] (S) b2
Section 215 [redacted] (S) b7E

Section 213 - Delayed Notice for Search Warrants - This is not a sunset provision, so we did not seek field input on this specific provision at this time.

Also - as you are aware, field offices collect statistics on their accomplishments (i.e. search warrants executed). I believe that Finance Division maintains, compiles, and reports these statistics. They may have more accurate field wide numbers.

I hope this is helpful.

[redacted] b2
Assistant General Counsel b6
Investigative Law Unit
Office of the General Counsel b7C
[redacted]

-----Original Message-----

From: [redacted] (Div00) (FBI)
Sent: Tuesday, May 18, 2004 1:41 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div00) (FBI)
Subject: Statistics re USA PATRIOT Act provisions
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

In anticipation of the Director's scheduled appearance before the Senate Judiciary Committee this Thursday, May 20th, we are trying to confirm the number of times we have used Delayed Notice (so-called "Sneak and Peek") Warrants, FISA Roving Wiretaps, and FISA Orders for Tangible Things (i.e., so-called Section 215 Orders), since passage of the USA PATRIOT Act.

I realize there are several potential complications with compiling such numbers (e.g., Delayed Notice Warrants used in traditional criminal cases, classification issues re 215 Orders, etc.). Nevertheless, if any of you could provide some input on this, it would be very helpful. We can almost guarantee the Director will be asked about the numbers when he testifies.

Is DOJ compiling numbers? Is there anyone at OLP or OIPR who may know?

Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:34 PM
To: [redacted] KC) (FBI)
Cc: [redacted] (Div09) (FBI)
Subject: 215 business record orders

CA# 05-CV-0845

b1
b2
b6
b6
b7C
b7C
b7E
b5

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I am an attorney in the National Security Law Branch of OGC, and I was discussing the issue of 215 orders with [redacted] She informed me that you'd written an EC in March indicating that you had used such orders [redacted] (S) wanted to clarify what you meant by that, inasmuch as we have never put a business record order application before the FISC, so I assume that you meant that you had submitted business record requests either to headquarters or to NSLB? Is that correct?

We are very close to getting such an order before the FISC, so if you have such request forms, and you haven't yet forwarded them to NSLB (and I don't think I have such requests), please do so and when the first order goes before the FISC and gets signed, we will then forward the rest that we have in the pipeline.

Thanks [redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

~~SECRET~~

CA# 05-CV-0845

[redacted] OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:52 PM
To: [redacted] (Div09) (FBI); [redacted] (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

I do not think the statistic report used by Finance would capture any FISA info (the info is classified). NSLB will assist you in obtaining the numbers of Roving FISAs and 215 requests As to delay notice, I do believe DOJ is maintaining these stats. I would call CTS, OEO or OLP.

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:03 PM
To: [redacted] (Div00) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

b6
b7C

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] I can provide you the results from the field survey that OGC conducted, however, I can also guarantee that these are not entirely accurate numbers. The field survey was voluntary, and the level of detail provided varied between the field offices. Furthermore, since then I have been advised that some HQ divisions have been utilizing various Patriot Act tools, and I did not receive any contributions from any HQ division on this survey, so their use is not included in any numbers that I have.

b1
b2
b7E

The field offices reported the following:

SECRET

Section 206 - Roving FISA orders [redacted] (S)
Section 215 - [redacted] (S)

Section 213 - Delayed Notice for Search Warrants - This is not a sunset provision, so we did not seek field input on this specific provision at this time.

Also - as you are aware, field offices collect statistics on their accomplishments (i.e. search warrants executed). I believe that Finance Division maintains, compiles, and reports these statistics. They may have more accurate field wide numbers.

I hope this is helpful.

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]
Assistant General Counsel
Investigative Law Unit
Office of the General Counsel
[redacted]

b2
b6
b7C

[redacted] (OGC) (FBI) b6

From: [redacted] (Div09) (FBI) b7C

Sent: Tuesday, May 18, 2004 3:00 PM

To: [redacted] Div09) (FBI)

Subject: FW: 215 business record orders

CA# 05-CV-0845

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

FYI ---- b6

-----Original Message-----

From [redacted] (KC) (FBI) b7C

Sent: Tuesday, May 18, 2004 2:50 PM

To: [redacted] (Div09) (FBI)

Subject: RE: 215 business record orders

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6

[redacted] b7C

Your assumption is correct, in that I was referring to filling out the forms and submitting them to NSLU for processing.

Thanks

[redacted]

-----Original Message-----

From [redacted] (Div09) (FBI) b6

Sent: Tuesday, May 18, 2004 1:34 PM b7C

To: [redacted] (KC) (FBI)

Cc: [redacted] (Div09) (FBI)

Subject: 215 business record orders

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b1 I am an attorney in the National Security Law Branch of OGC, and I was discussing the issue of 215 orders
b2 with [redacted] She informed me that you'd written an EC in March indicating that you had used such orders
[redacted] I wanted to clarify what you meant by that, inasmuch as we have never put a business record
b6 order application before the FISC, so I assume that you meant that you had submitted business record (S)
b7C requests either to headquarters or to NSLB? Is that correct?

b7E We are very close to getting such an order before the FISC, so if you have such request forms, and you haven't yet forwarded them to NSLB (and I don't think I have such requests), please do so and when the first order goes before the FISC and gets signed, we will then forward the rest that we have in the pipeline.

Thanks [redacted] b6

b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OCA) (FBI) b6
Sent: Friday, June 18, 2004 3:57 PM b7C
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OCA) (FBI)

UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

The attached email includes DOJ's draft response to Sen. Feinstein's correspondence re the provisions of the USA PATRIOT Act (USAPA) due to expire in 2005.

As you can see, the draft letter mentions an "attached report" as well as "further examples" to be provided in a "classified form."

I have asked DOJ for a copy of the "attached report," but I have not received it. Based on your voicemail, I suspect the final version of DOJ's response may have omitted the reference to an attached report, in favor of a classified report to be provided at some future date. As I understand it, you've been asked to help prepare such a report, with classified examples of situations in which the relevant USAPA provisions were used.

I believe [redacted] in OGC has been trying to collect such examples from the Field. She and [redacted] may be your best contacts on this issue. I'm also happy to assist in any way I can.

I hope this helps. If I learn more from DOJ, I'll let you know. b6 b7C

[redacted]
OCA b2 b6 b7C

UNCLASSIFIED

[redacted] (OGC) (FBI)

b6
b7C

From: ExecSec (RMD)
Sent: Thursday, June 24, 2004 6:57 AM
To: [redacted] (CTD) (FBI); [redacted] (CTD) (FBI); [redacted] (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI)
Subject: TRIM Document : DOJ/EXECSEC/04/DO/3062 : Following up on her 6/4/04 conversation with AG & her 3/23 & 4/28/04 ltrs (encl) requests comprehensive review of implementation, value & importance of 16 provisions of USA PATRIOT Act subject to sunset provisions.

Following up on her 6404 conve...

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-11-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

INFORMATION ONLY: OCA, CTD, and OGC

Instructions:

Attached is correspondence referred to the FBI by the U.S. Department of Justice (DOJ) Executive Secretariat, FOR INFORMATION ONLY. IT DOES NOT REQUIRE ANY FBI ACTION; however, it is being referred to you for your information in the event you may be contacted by the DOJ entity tasked with handling the response. The original will be forwarded to the Records Management Centers Unit for uploading into ACS.

If this matter needs to be reassigned to another entity, the FBI ExecSec should be advised immediately (within 2 days of e-mail receipt). The ExecSec will need to know to whom the request should be reassigned to, together with a point of contact (if known).

If you have any questions, comments, suggestions, or require the attached correspondence to be sent to another division/office for action or information, please contact the Executive Secretariat, [redacted] or by e-mail to ExecSec.

b2
b6
b7C

------< TRIM Record Information >------

Date Due :
Action Office :
Current Action :
All Contacts : Kelley, Patrick (Info); Bald, Gary (Info); Kalisch, Eleni (Info)
Access DB or Workflow : 605053
From : FEINSTEIN, DIANNE
Constituent :
Title (Free Text Part) : Following up on her 6/4/04 conversation with AG & her 3/23 & 4/28/04 ltrs (encl) requests comprehensive review of implementation, value & importance of 16 provisions of USA PATRIOT Act subject to sunset provisions. See WFS 582542 & 558986. (PM)
Date of Communication : Monday, June 14, 2004
Notes :
Related Records : 04/DO/1529: Advises that USA PATRIOT ACT is a critical tool in the nation's fight against terrorism. Expresses concern with tone of discussions about the Act and the 16 provisions set to expire in 2005. Requests DOJ & CIA ensure review of the 16 provisions. (PM) (Related to); 04/DO/2308: Regarding her unanswered request, dated 3/23/04, for a comprehensive review of the implementation, value and importance of each of the 16 provisions of the USA PATRIOT ACT subject to "sunset" provisions. See WF 558986. (PM) (Related to)

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Friday, July 02, 2004 2:38 PM b7C
To: [redacted] (KX) (FBI)
Subject: Sunset provisions

CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S) [redacted] I am updating some of the examples we've used to justify the Patriot Act. In your 3/18 EC, you noted that [redacted] has [redacted] Section 214 [redacted] Can you provide me any further information on this pen/trap order? (i.e. file #) This may be a perfect example for us to help respond to some specific Congressional concerns.

Thanks in advance for your help. If you have any questions, please feel free to contact me.

Have a good 4th!

[redacted]
Assistant General Counsel
Investigative Law Unit
Office of the General Counsel
[redacted]

b1
b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] (OGC) (FBI)

CA# 05-CV-0845

From: [redacted] (OGC) (FBI) b6

Sent: Tuesday, July 13, 2004 9:32 AM b7C

To: [redacted] OCA) (FBI)

Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (CTD) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI)

Subject: Examples for Patriot Act Sunset Provisions

UNCLASSIFIED
NON-RECORD

[redacted] As per our conversation, the following are the sunset provisions of the Patriot Act where I do not have many examples addressing our use of such provision. b6

Sections 201 & 202 - Expanded predicate offenses for Title III b7C

Section 204 - Clarification of intelligence exceptions - (I am hoping that NSLB can offer input here)

Section 207 - Extended duration for FISAs - (I believe that NSLB was collecting examples for this provision.)

Section 209 - Obtaining voice mail with a search warrant

Section 223 & 225 - addressing civil liability issues (I don't anticipate that there are any examples to cite for these provisions)

I am in the process of going through the examples that CTD provided to me, however, it will take additional discussions with CTD before I can determine how the Patriot Act provisions were utilized in most of these cases.

I hope this is helpful, and I look forward to discussing this further in our meeting later this morning.

[redacted] b2
ILU/OGC
[redacted] b6
b7C

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI) b6
Sent: Tuesday, May 18, 2004 3:01 PM b7C
To: [redacted] (Div09) (FBI) CA# 05-CV-0845
Subject: RE: 215 business record orders

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Thanks - I'll update the survey summary that I have. Are you going to advise [redacted]

-----Original Message-----
From: [redacted] (Div09) (FBI) b6
Sent: Tuesday, May 18, 2004 3:00 PM b7C
To: [redacted] (Div09) (FBI)
Subject: FW: 215 business record orders

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

FYI ----
-----Original Message-----
From: [redacted] (KC) (FBI)
Sent: Tuesday, May 18, 2004 2:50 PM
To: [redacted] (Div09) (FBI)
Subject: RE: 215 business record orders

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

SENSITIVE BUT UNCLASSIFIED b6
NON-RECORD b7C

[redacted]

Your assumption is correct, in that I was referring to filling out the forms and submitting them to NSLU for processing.

Thanks

[redacted] b1

-----Original Message----- b2
From: [redacted] (Div09) (FBI) b6
Sent: Tuesday, May 18, 2004 1:34 PM b7C
To: [redacted] (KC) (FBI) b7E
Cc: [redacted] (Div09) (FBI)
Subject: 215 business record orders

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I am an attorney in the National Security Law Branch of OGC, and I was discussing the issue of 215 orders with [redacted] She informed me that you'd written an EC in March indicating that you had used such orders [redacted] wanted to clarify what you meant by that, inasmuch as we have never put a business record order application before the FISC, so I assume that you meant that you had

(S)

submitted business record requests either to headquarters or to NSLB? Is that correct?

We are very close to getting such an order before the FISC, so if you have such request forms, and you haven't yet forwarded them to NSLB (and I don't think I have such requests), please do so and when the first order goes before the FISC and gets signed, we will then forward the rest that we have in the pipeline.

Thanks [redacted] b6 b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI) b6
Sent: Friday, May 21, 2004 9:04 AM b7C CA# 05-CV-0845
To: [redacted] (Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

UNCLASSIFIED
NON-RECORD

Thanks for the update. I was not aware that the number of roving taps would be classified.

-----Original Message-----
From: [redacted] (Div00) (FBI)
Sent: Tuesday, May 18, 2004 7:19 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions b6 b7C

UNCLASSIFIED
NON-RECORD

(S) I spoke with [redacted] @ DOJ OLP. She advised as follows:
Delayed Notice - use [redacted] although this is an old number and should be updated. She was not aware that it had been updated.
Roving Wiretaps - # is classified
215 Requests - # (0) was declassified in Sept '03, but has not been declassified since. In [redacted] opinion it is still classified.

If NSLB has additional data that would be helpful for the Director's background information, it would be appreciated. Thanks,

b1 b2 b6 b7C b7E

[redacted]
Special Counsel
Office of Congressional Affairs
[redacted]

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:52 PM
To: [redacted] (Div09) (FBI); [redacted] (Div00) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions b6 b7C

UNCLASSIFIED
NON-RECORD

I do not think the statistic report used by Finance would capture any FISA info (the info is classified). NSLB will assist you in obtaining the numbers of Roving FISAs and 215 requests As to delay notice, I do believe DOJ is maintaining these stats. I would call CTS, OEO or OLP.

-----Original Message-----

From: (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:03 PM
To: Div00) (FBI) (Div09) (FBI)
I. (Div09) (FBI); (Div09) (FBI)
Cc: Div00) (FBI) b6
Subject: RE: Statistics re USA PATRIOT Act provisions b7C

UNCLASSIFIED
NON-RECORD

I can provide you the results from the field survey that OGC conducted, however, I can also guarantee that these are not entirely accurate numbers. The field survey was voluntary, and the level of detail provided varied between the field offices. Furthermore, since then I have been advised that some HQ divisions have been utilizing various Patriot Act tools, and I did not receive any contributions from any HQ division on this survey, so their use is not included in any numbers that I have. b6 b7C

The field offices reported the following:

Section 206 - Roving FISA orders (S)
Section 215 (S)

Section 213 - Delayed Notice for Search Warrants - This is not a sunset provision, so we did not seek field input on this specific provision at this time.

Also - as you are aware, field offices collect statistics on their accomplishments (i.e. search warrants executed). I believe that Finance Division maintains, compiles, and reports these statistics. They may have more accurate field wide numbers.

I hope this is helpful.

b1
b2
b7E

DATE: 12-04-2005
CLASSIFIED BY 65179 DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b2
b6
b7C

Assistant General Counsel
Investigative Law Unit
Office of the General Counsel

-----Original Message-----
From: Div00) (FBI)
Sent: Tuesday, May 18, 2004 1:41 PM
To: BOWMAN, MARION E. (Div09) (FBI); (Div09) (FBI); (Div09) (FBI) Div09) (FBI)
Cc: Div00) (FBI)
Subject: Statistics re USA PATRIOT Act provisions
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

In anticipation of the Director's scheduled appearance before the Senate Judiciary Committee this Thursday, May 20th, we are trying to confirm the number of times we have used Delayed Notice (so-called "Sneak and Peek") Warrants, FISA Roving Wiretaps, and FISA Orders for Tangible Things (i.e., so-called Section 215 Orders), since passage of the USA PATRIOT Act.

I realize there are several potential complications with compiling such numbers (e.g., Delayed

Notice Warrants used in traditional criminal cases, classification issues re 215 Orders, etc.). Nevertheless, if any of you could provide some input on this, it would be very helpful. We can almost guarantee the Director will be asked about the numbers when he testifies.

Is DOJ compiling numbers? Is there anyone at OLP or OIPR who may know?

Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] OGC) (FBI)
Sent: Tuesday, June 01, 2004 4:04 PM
To: [redacted] (SD) (FBI)
Subject: RE: Patriot Act stats

b6
b7C

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] here are no clear and complete Patriot Act stats available at this time. However, you might consider checking the director's testimony on the Hill. (most recently on 5/20). He does mention our use of the Patriot Act.

Many of the statistics I'm compiling would be considered classified because they involve the use of FISAs or other national security related tools.

DOJ has released some documents to the Hill. You might consider looking at their website.

The congressional research service compiled a legal analysis on the sunset provisions. No stats, but some helpful documentation on the various provisions. You can probably find it on their website. Charles Doyle was that author. Report was dated January 2, 2004.

I wish I had something better to point you to, but unfortunately there just isn't that I'm aware of. If there is a specific question you have for a specific reason, I might be able to get the answer for you.

Hope that helps. Feel free to call me if I can do something more for you.

b2
[redacted]
b6
Assistant General Counsel
Investigative Law Unit
Office of the General Counsel
b7C
[redacted]

-----Original Message-----
From: [redacted] (SD) (FBI)
Sent: Monday, May 24, 2004 12:16 PM
To [redacted] (Div09) (FBI)
Subject: Patriot Act stats

b6
b7C

UNCLASSIFIED
NON-RECORD

b6

Hi [redacted]

b7C

I am inquiring as to Patriot Act stats. Have they been compiled and, if so, where might I find them? I am looking for some light reading.

Thanks for your help.

b2
b6
[redacted]
b7C

UNCLASSIFIED

UNCLASSIFIED

[redacted] OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Tuesday, June 22, 2004 12:01 PM b7C CA# 05-CV-0845
To: [redacted] (CI) (FBI)
Subject: RE: Sunset Provisions - Roving FISA order

DATE: 12-04-2005
CLASSIFIED BY 12-04-2005 65179/DMH/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-04-2030

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I'm making final revisions to my summary of examples where we used the various Sunset provisions found in the Patriot Act. As you may recall, you had responded that the Section 206 [redacted] Now that there has been a public indictment and press release on this case, how would you like me to cover this example? I'm suggesting that we include specifics from the press release, but keep it classified since [redacted] Am I correct?

Thanks for your input. -[redacted] b2 b6 b7C b5

-----Original Message-----
From: [redacted] (CI) (FBI) b7C b6
Sent: Monday, May 03, 2004 1:20 PM
To: [redacted] (Div09) (FBI) b7C
Subject: RE: Sunset Provisions - Roving FISA order

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S) [redacted] (S)

JT

-----Original Message-----
From: [redacted] (Div09) (FBI) b1 b6 b7C
Sent: Friday, April 30, 2004 12:07 PM
To: [redacted] (CI) (FBI)
Subject: FW: Sunset Provisions - Roving FISA order b6 b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

-----Original Message-----
From: [redacted] (Div09) (FBI) b6
Sent: Friday, April 30, 2004 12:03 PM
To: [redacted] (CI) (FBI) b7C
Subject: Sunset Provisions - Roving FISA order

SENSITIVE BUT UNCLASSIFIED

NON-RECORD

[redacted] hanks for your response to our call to the field for examples using the sunset provisions. I'm compiling the results for the GC. In your EC, you noted that the [redacted] Can I get more info on this use? It seems like a good case to include as an example. Also let me know how you want it classified. You noted it was still an ongoing case, so should we classify it? or just label it law enforcement sensitive?

Thanks.

[redacted]

b2
b6
b7A
b7C
b7E

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Tuesday, June 22, 2004 12:04 PM
To: [redacted] (OGC) (FBI) b7C
Subject: RE: Sunset Provisions - Section 207 - Extended FISAs for non-US persons

UNCLASSIFIED
NON-RECORD

[redacted] I'm trying to finalize the summary of field input on the sunset provisions. Does NSLB have anything to provide on Section 207 regarding extended FISAs for non-US persons? Thanks.

b6
b7C

As promised, when I complete the draft, I'll forward a copy to you.

Thanks again for any help NSLB can provide.

[redacted] b6
b7C

-----Original Message-----
From: [redacted] (Div09) (FBI) b6
Sent: Friday, April 30, 2004 12:50 PM
To: [redacted] Div09) (FBI) b7C
Subject: RE: Sunset Provisions - Section 207 - Extended FISAs for non-US persons

UNCLASSIFIED
NON-RECORD

I'll forward this to the units and get any info we have. Thanks.

-----Original Message-----
From: [redacted] (Div09) (FBI) b6
Sent: Friday, April 30, 2004 12:45 PM
To: [redacted] (Div09) (FBI) b7C
Subject: Sunset Provisions - Section 207 - Extended FISAs for non-US persons

UNCLASSIFIED
NON-RECORD

[redacted] Somehow I missed section 207 when I sent out the EC seeking input from the field on the sunset provisions. This provision amended the time lines for FISA orders for agents of a foreign power. (extending the initial ELSUR orders to 120 days with 1 year renewals, and various timelines for physical searches depending on the target). Does NSLB have language or examples to use to support the renewal of this provision?

b6
b7C

thanks in advance for your help.

[redacted] b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 227
Page 18 ~ Duplicate
Page 19 ~ Duplicate
Page 20 ~ Duplicate
Page 21 ~ Duplicate
Page 22 ~ Duplicate
Page 23 ~ Duplicate
Page 24 ~ Duplicate
Page 25 ~ Duplicate
Page 26 ~ Duplicate
Page 27 ~ Duplicate
Page 28 ~ Duplicate
Page 29 ~ Duplicate
Page 30 ~ Duplicate
Page 31 ~ Duplicate
Page 32 ~ Duplicate
Page 33 ~ Duplicate
Page 34 ~ Duplicate
Page 35 ~ Duplicate
Page 36 ~ Duplicate
Page 37 ~ Duplicate
Page 38 ~ Duplicate
Page 39 ~ Duplicate
Page 40 ~ Duplicate
Page 41 ~ Duplicate
Page 42 ~ Duplicate
Page 43 ~ Duplicate
Page 44 ~ Duplicate
Page 45 ~ Duplicate
Page 46 ~ Duplicate
Page 47 ~ Duplicate
Page 48 ~ Duplicate
Page 49 ~ Duplicate
Page 50 ~ Duplicate
Page 51 ~ Duplicate
Page 52 ~ Duplicate
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 55 ~ Duplicate
Page 56 ~ Duplicate
Page 57 ~ Duplicate
Page 58 ~ Duplicate
Page 59 ~ Duplicate
Page 60 ~ Duplicate
Page 61 ~ Duplicate

Page 62 ~ Duplicate
Page 63 ~ Duplicate
Page 64 ~ Duplicate
Page 65 ~ Duplicate
Page 66 ~ Duplicate
Page 67 ~ Duplicate
Page 68 ~ Duplicate
Page 69 ~ Duplicate
Page 70 ~ Duplicate
Page 71 ~ Duplicate
Page 72 ~ Duplicate
Page 73 ~ Duplicate
Page 74 ~ Duplicate
Page 75 ~ Duplicate
Page 76 ~ Duplicate
Page 77 ~ Duplicate
Page 78 ~ Duplicate
Page 79 ~ Duplicate
Page 80 ~ Duplicate
Page 81 ~ Duplicate
Page 82 ~ Duplicate
Page 83 ~ Duplicate
Page 207 ~ Duplicate
Page 208 ~ Duplicate
Page 209 ~ Duplicate
Page 210 ~ Duplicate
Page 211 ~ Duplicate
Page 212 ~ Duplicate
Page 213 ~ Duplicate
Page 214 ~ Duplicate
Page 215 ~ Duplicate
Page 216 ~ Duplicate
Page 217 ~ Duplicate
Page 218 ~ Duplicate
Page 219 ~ Duplicate
Page 220 ~ Duplicate
Page 221 ~ Duplicate
Page 222 ~ Duplicate
Page 223 ~ Duplicate
Page 224 ~ Duplicate
Page 225 ~ Duplicate
Page 226 ~ Duplicate
Page 227 ~ Duplicate
Page 228 ~ Duplicate
Page 229 ~ Duplicate
Page 230 ~ Duplicate
Page 231 ~ Duplicate
Page 232 ~ Duplicate
Page 233 ~ Duplicate
Page 234 ~ Duplicate
Page 235 ~ Duplicate

Page 236 ~ Duplicate
Page 237 ~ Duplicate
Page 238 ~ Duplicate
Page 239 ~ Duplicate
Page 240 ~ Duplicate
Page 241 ~ Duplicate
Page 242 ~ Duplicate
Page 243 ~ Duplicate
Page 244 ~ Duplicate
Page 245 ~ Duplicate
Page 246 ~ Duplicate
Page 247 ~ Duplicate
Page 248 ~ Duplicate
Page 249 ~ Duplicate
Page 250 ~ Duplicate
Page 251 ~ Duplicate
Page 252 ~ Duplicate
Page 253 ~ Duplicate
Page 254 ~ Duplicate
Page 255 ~ Duplicate
Page 256 ~ Duplicate
Page 285 ~ Duplicate
Page 286 ~ Duplicate
Page 287 ~ Duplicate
Page 288 ~ Duplicate
Page 289 ~ Duplicate
Page 290 ~ Duplicate
Page 291 ~ Duplicate
Page 292 ~ Duplicate
Page 293 ~ Duplicate
Page 294 ~ Duplicate
Page 295 ~ Duplicate
Page 296 ~ Duplicate
Page 297 ~ Duplicate
Page 298 ~ Duplicate
Page 299 ~ Duplicate
Page 300 ~ Duplicate
Page 301 ~ Duplicate
Page 302 ~ Duplicate
Page 303 ~ Duplicate
Page 304 ~ Duplicate
Page 305 ~ Duplicate
Page 306 ~ Duplicate
Page 314 ~ Duplicate
Page 315 ~ Duplicate
Page 316 ~ Duplicate
Page 317 ~ Duplicate
Page 318 ~ Duplicate
Page 319 ~ Duplicate
Page 321 ~ Duplicate
Page 322 ~ Duplicate

Page 323 ~ Duplicate
Page 324 ~ Duplicate
Page 326 ~ Duplicate
Page 327 ~ Duplicate
Page 328 ~ Duplicate
Page 329 ~ Duplicate
Page 330 ~ Duplicate
Page 331 ~ Duplicate
Page 332 ~ Duplicate
Page 341 ~ Duplicate
Page 367 ~ Duplicate
Page 368 ~ Duplicate
Page 374 ~ Duplicate
Page 378 ~ Duplicate
Page 379 ~ Duplicate
Page 380 ~ Duplicate
Page 381 ~ Duplicate
Page 382 ~ Duplicate
Page 383 ~ Duplicate
Page 384 ~ Duplicate
Page 385 ~ Duplicate
Page 386 ~ Duplicate
Page 387 ~ Duplicate
Page 388 ~ Duplicate
Page 389 ~ Duplicate
Page 390 ~ Duplicate
Page 391 ~ Duplicate
Page 392 ~ Duplicate
Page 393 ~ Referral/Direct
Page 394 ~ Referral/Direct
Page 396 ~ Referral/Direct
Page 397 ~ Referral/Direct
Page 398 ~ Referral/Direct
Page 399 ~ Referral/Direct
Page 400 ~ Referral/Direct
Page 401 ~ Referral/Direct
Page 402 ~ Referral/Direct
Page 403 ~ Referral/Direct
Page 404 ~ Referral/Direct
Page 405 ~ Referral/Direct
Page 406 ~ Duplicate
Page 407 ~ Duplicate
Page 408 ~ Duplicate
Page 409 ~ Duplicate
Page 410 ~ Duplicate
Page 411 ~ Duplicate
Page 412 ~ Duplicate
Page 413 ~ Duplicate
Page 414 ~ Duplicate
Page 415 ~ Duplicate
Page 417 ~ Referral/Direct

Page 418 ~ Referral/Direct
Page 419 ~ Referral/Direct
Page 420 ~ Referral/Direct
Page 421 ~ Referral/Direct
Page 422 ~ Referral/Direct
Page 423 ~ Referral/Direct
Page 424 ~ Referral/Direct
Page 425 ~ Referral/Direct
Page 426 ~ Referral/Direct
Page 427 ~ Referral/Direct
Page 428 ~ Referral/Direct
Page 429 ~ Referral/Direct
Page 430 ~ Referral/Direct
Page 431 ~ Referral/Direct
Page 432 ~ Referral/Direct
Page 433 ~ Referral/Direct
Page 434 ~ Referral/Direct
Page 435 ~ Referral/Direct
Page 436 ~ Referral/Direct
Page 437 ~ Referral/Direct
Page 438 ~ Referral/Direct
Page 439 ~ Referral/Direct
Page 440 ~ Referral/Direct
Page 441 ~ Referral/Direct
Page 442 ~ Referral/Direct
Page 443 ~ Referral/Direct
Page 444 ~ Referral/Direct
Page 445 ~ Referral/Direct
Page 446 ~ Referral/Direct
Page 447 ~ Referral/Direct

USA Patriot Act

Selected provisions

Information Sharing: Section 203

- Amends FRCP 6(e) and 18 U.S.C. 2517 (Title III) to permit disclosure of specified categories of FGJ and T-3 information to specified recipients for specified uses.
- Heretofore, such disclosures were prohibited by law except in very rare circumstances.

Section 203: Information Subject to Disclosure

- Foreign Intelligence
  - Foreign government capabilities and intentions
  - International terrorist activities
  - Information related to U.S. defensive capability
- Counterintelligence
  - Espionage
  - Sabotage

Section 203: Authorized Recipients and Uses

- Specified Recipients – "any Federal law enforcement, national defense, or national security official . . ."
- Specified Uses – "for performance of official duties and subject to any limitations on the unauthorized disclosure of such information."

Section 203: Notice requirements

- FGJ Information: AUSA must file notice under seal within reasonable time to the court that information was disclosed and to whom
- No notice requirement for Title III information

Section 203 (d) HSA Amendment

- Expands authorized recipients to include "any federal, state, local, or foreign government official for the purpose of preventing or responding to" terrorism threats
- Disclosure must be consistent with DCI obligation to protect intelligence sources and methods and AG obligation to protect sensitive law enforcement information

Information Sharing Section 905(a)

- Requires expeditious disclosure of foreign intelligence acquired during course of a criminal investigation to the DCI
- Mandatory, not permissive
- Permits AG to establish exceptions in consultation with DCI to protect significant law enforcement interests

Section 905(b)

- AG, in consultation with DCI, to develop guidelines to ensure timely responses to IC reports of criminal activity by source
- Responses must provide notice to DCI of AG's intention to commence or decline to commence criminal investigation into reported activity

Section 212

- Emergency disclosure of electronic communications
- Danger of death or serious physical injury
- Service Provider's discretion
- FBI can initiate the emergency predicate
- Reporting requirement

Section 215

- FISA Court order to seize tangible things
- Tangible things could include business records
- Standard: relevance to a foreign intelligence or international terrorism investigation
- "No notice" provision

Section 217

- Computer Trespasser Provision
- Definition – person who accesses a protected computer system w/o authorization
- Does not include existing customer even if customer is using unauthorized entry
- Interception w/o court order permitted subject to conditions

The Latest Controversy: Section 314

- Permits financial institutions and law enforcement agencies to share information
  - LE > FI = suspicious customers
  - FI > LE = verify existence of accounts
  - FI > FI = share information
- Process set forth in 31 C.F.R. § 103.100
- All requests through FinCEN, which distributes requests to FIs every two weeks

Section 314 (continued)

- Predicate offenses:
  - Terrorism; or
  - Money Laundering
- Investigation must be significant
- Information must be essential
- Section 314 only identifies accounts.
- Traditional legal process required to obtain records from those accounts

Patriot Act Sections Reaching out to Foreign Banks

- Under § 318, foreign banks are now included within the definition of a "financial Institution"
- This means that, if a subject launders money through a foreign bank, it constitutes money laundering under 18 U.S.C. §§ 1956, 1957—assuming the other elements of those violations are satisfied

Foreign Banks (continued)

- § 317 creates "long-arm" jurisdiction offenses involving a foreign bank with a correspondent bank account in the U.S.
- The effect of this is to give the U.S. jurisdiction against the bank and its assets in a civil money laundering action under 18 U.S.C. § 1956
- § 317 also permits a court to enter restraining orders and appoint receivers for any of the bank's assets in the U.S.

Patriot Act Forfeiture (continued)

- § 323 corrects two major flaws in U.S. law (28 U.S.C. § 2467) that permits the AG to enforce a foreign forfeiture judgment by forfeiting property in the U.S.
  - 1) The property in question can now be preserved through an uncontestable U.S. court restraining order
  - 2) Applies to foreign forfeiture order based on any violation of foreign law that would also permit forfeiture under U.S. law

Miscellaneous Provisions

- 214 – Pens and T & T for FISA
- 216 – Nationwide jurisdiction for Pens and T & T
- 220 – Nationwide jurisdiction for search warrants for electronic evidence
- 802 – Amends 18 U.S.C. § 2331 by defining "domestic terrorism" as another form of terrorism that occurs primarily within the U.S.

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 10/26/2001

To: All Divisions **Attn:** ADIC, SAC
CDC

b2

From: Office of the General Counsel
NSLU/NSLB, Room 7975
Contact: National Security Law Unit, [redacted]

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E
[redacted]

Drafted By: [redacted] mjw

b6
b7C

Case ID #: 66F-HQ-A1247863 (None)

Title: NEW LEGISLATION
REVISIONS TO FCI/IT LEGAL AUTHORITIES
FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

Synopsis: Summarizes recent changes to FISA statute and related legal authorities.

Details:

Background

On October 26, 2001, the President signed the "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" which significantly revises many legal authorities relating to counterterrorism. The Act, which consists of more than 150 sections, effects changes in national security authorities, the substantive criminal law, immigration law, money laundering statutes, victim assistance statutes, and other areas. The National Security Law Unit, OGC, is issuing guidance on those portions of the Act relating to national security operations. This communication addresses changes in the Foreign Intelligence Surveillance Act of 1978 (FISA) and certain other statutes relating to information sharing; a related serial describes changes to National Security Letter authorities. Other OGC communications address the non-national security law portions of the Act.

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ-A1247863, 10/26/2001

In the wake of the September 11, 2001 attacks, the Administration proposed to Congress a variety of proposals to increase the efficiency and effectiveness of FCI/IT operations, and a substantial portion of the Act is given over to this purpose. In particular, the Act seeks to improve the efficiency of the FISA process and to remove barriers to the timely sharing of information between FCI/IT intelligence operations and criminal investigations.

Many provisions of the Act, including most of the national security provisions, are subject to the "sunset" provision described in Section 224 of the Act. This Section states that the authorities expire on December 31, 2005. At that time, Congress will have to decide whether or not to re-authorize the provisions.

The following summarizes the changes in national security authorities by various sections in the Act (A separate EC of this same date addresses changes to National Security Letter (NSL) authorities). For each section, there is a summary of potential changes in FBI operational procedures. Recipients should note that this is only initial guidance; more detailed explanations and procedures may follow in subsequent communications.

1. Sharing Grand Jury, Title III and Criminal Investigative Information

Section 203 first amends Federal Rule of Criminal Procedure 6(e) to permit the disclosure of grand jury information involving intelligence information "to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section also requires subsequent notice to the Court of the agencies to which information was disseminated and adds a definition of "foreign intelligence information" to Rule 6(e). The Grand Jury portion of this Section (Section 203(a)) is not subject to the sunset provision.

Section 203 then amends Title III to allow the same sort of disclosure of Title III information when the matters involve foreign intelligence "to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." The Section adds a definition of foreign intelligence information to Title III, and requires the Attorney

General to develop procedures for the sharing of Grand Jury or Title III information that identifies a U.S. person.

Finally, Section 203 establishes that "notwithstanding any other law" it is lawful for criminal investigators to share foreign intelligence information obtained in the course of a criminal investigation with any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official, as above.

The intent of Section 203 is to eliminate barriers to the timely sharing of information between criminal investigators and other entities (the Intelligence Community, the INS, DoD, etc.) involved in the protection of the national security. The Section essentially gives the FBI full discretion to share criminal investigative information, regardless of its source, whenever it involves foreign intelligence information (which is defined to include all foreign intelligence, counterintelligence, and counterterrorism information).

Procedural Changes: FBI components in possession of information obtained through criminal investigative techniques that is also foreign intelligence information should arrange for the appropriate dissemination of the information. Dissemination to the Intelligence Community must be coordinated through the relevant NSD or CTD units at FBIHQ. When the DOJ issues procedures relating to the dissemination of U.S. person information, the field will receive additional guidance.

2. "Roving" FISA ELSUR Authority

b1

Section 206 amends FISA to allow the Court to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in tradecraft designed to defeat ELSUR such as by [redacted] (S) the Court can issue an order directing "other persons," [redacted] etc., to effect the authorized electronic surveillance. (S) Even if the target is not engaged in obvious tradecraft, we can obtain such an order as long as the target's actions may have the effect of thwarting surveillance. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. [redacted]

b5

Procedural Changes: When the field wants to obtain roving ELSUR authority, the request for a FISA sent to FBIHQ should include specific facts that will allow the Court to find that the actions of the target may have the effect of thwarting the requested surveillance, absent the roving authority. [redacted] b2 b5 b7E

[redacted] DOJ/OIPR may issue more detailed guidance as experience with this provision grows.

3. Changes in the Duration of FISA Authority

Section 207 extends the standard duration for several categories of FISA orders. First, the section allow for ELSUR and search orders on non-U.S. person agents of a foreign power pled under Section 101(b)(1)(A) of FISA (i.e., officers and employees of foreign powers, including members of international terrorist groups) to run for an initial period of 120 days (instead of 90) and to be renewed for periods of one year. The section also extends the standard duration of physical search orders in all other cases (U.S. persons and non-officer/employee targets) from 45 to 90 days.

Procedural Changes: None are required. OIPR will transition existing coverages to the new durations as they come up for renewal.

4. Expansion of the FISA Court

In order to increase the availability of FISA judges, Section 207 expands the Court from seven judges to eleven judges, three of whom must reside in the Washington, D.C. area.

Procedural Changes: None are required.

5. Changes in FISA Pen Register/Trap and Trace Authority

Section 214 makes a substantial revision to the standard for a FISA pen register/trap and trace. Prior to the Act, FISA pen registers required two showings: (1) relevance to an investigation, and (2) specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. Section 214 simply eliminates the second of the required showings. FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign

intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

b1
b5

This new standard requires that the information sought be relevant to an "ongoing investigation to protect against international terrorism or clandestine intelligence activities." Use of this technique is authorized [redacted] (S)

[redacted] (S)

[redacted] Although the language differs somewhat from that used in the previous versions of the statute, [redacted] b5

The Section also inserts the language "provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States." Congress inserted this to indicate that the technique will not be used against U.S. persons who are merely exercising constitutionally protected rights. b5

[redacted]

[redacted] b5

[redacted] For example, information concerning apparent associates or, or individuals in contact with, the subject of a investigation, may be relevant.

Procedural Changes: None are required. The field may continue to request FISA pen register/trap and trace authority through FBIHQ in the established manner. However, the requests now need only contain a brief statement explaining the nature of the investigation and the relevance to that investigation of the information sought through the pen register. NSLU and OIPR will

develop additional guidance streamlining the process for requesting this authority.

6. Changes in FISA Business Records Authority

Section 215 changes the business records authority found in Title V of FISA. The old language allowed the FISA Court to issue an order compelling the production of certain defined categories of business records (the records of common carriers, public accommodations, vehicle rentals, and storage facilities) upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. Section 215 changes this standard to simple relevance (just as in the FISA pen register standard described above) and gives the Court the authority to compel production of "any tangible things (including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This is the same standard described above for Section 214.

In the past, the FBI has encountered situations in which the holders of relevant records refused to produce them absent a subpoena or other compelling authority. When those records did not fit within the defined categories for National Security Letters or the four categories then defined in the FISA business records section, the FBI had no means of compelling production. With the new language the FBI can seek a FISA court order for any such materials.

Procedural Changes: None are required. The field may continue to request business records orders through FBIHQ in the established manner. However, such requests may now seek production of any relevant information, and need only contain information establishing such relevance. NSLU and OIPR will develop additional guidance streamlining the process for requesting this authority.

7. Changes to "Primary Purpose" Standard in FISA

Sections 218 and 504 clarify the "primary purpose" issue in the FISA statute. In its prior form, the FISA required a certification that foreign intelligence be "the" purpose of the requested authority. The FISA Court interpreted this to mean that foreign intelligence, as opposed to criminal prosecution,

had to be the "primary" purpose of the requested authority. Thus, interaction between FBI personnel involved in a FISA and criminal prosecutors could call into question the primary intelligence purpose of the FISA (by indicating a purpose different from foreign intelligence). As a result, FISA pleadings have often contained detailed accounts of all communication with criminal prosecutors in cases involving FISA.

Section 218 changes FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amends FISA to allow that personnel involved in a FISA may consult with law enforcement officials to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose."

These changes are meant to allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk. As such, these changes address extraordinarily complex issues that have long occupied the FISA Court and DOJ. FBIHQ expects that DOJ shortly will issue revised policy on these topics.

Procedural Changes: None are required at present. The field should be aware that greater consultation with prosecutors is now possible, but, given the continuing uncertainty surrounding these issues, should continue to coordinate such consultation through FBIHQ. Additional guidance will be issued.

8. Civil Liability for Unauthorized Disclosure

Section 223 establishes civil liability for certain unauthorized disclosures, including unauthorized disclosures of FISA information. In reference to FISA, this is simply an expansion of existing civil liability, and should not significantly affect operations (since unauthorized disclosure of FISA information is already subject to more severe criminal penalties).

Procedural Changes: None are required. OGC may issue a more detailed analysis of this provision at a later date.

9. Immunity for Compliance with FISA

Section 225 grants providers of wire or electronic communication service, landlords, custodians, and other persons with immunity from civil liability for complying with the requirements of FISA. This provision simply clarifies that

To: All Divisions From: Office of the General Counsel
Re: 66F-HQ-A1247863, 10/26/2001

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in FCI/IT operations and to other division personnel as appropriate.

♦♦

National Security Law: Developments 2001-2002

[redacted]

National Security Law Unit, OGC

CDC Conference, January 8, 2002

b6
b7C

Today's Presentations

- Review of Legislative Developments
  - Intelligence Authorization Act for FY2001
  - USA PATRIOT Act
  - Intelligence Authorization Act for FY2002
- Information Sharing, Accuracy Policies
- National Security Letters
- Attorney General Guidelines Revisions
- FISA Unit

In Congress

- Senate passed version close to the Administration's draft (USA Act)
- House version substantially different, but substituted at last minute for something like the Senate version
- House insisted on "sunset" provision
- House passes PATRIOT Act
- Conference, then USA PATRIOT Act passed
- President signed on October 26, 2001

Structure of the Act

- National Security Stuff
  - Title II: "Enhanced Surveillance Procedures"
  - Title V: "Removing Obstacles to Investigating Terrorism"
- Other titles address money laundering, immigration, substantive criminal law
- Other stuff

Section 204: Sharing of criminal information with IC

- 204 amends Rule 6(e), Title III to allow sharing of Title III and GJ information:
  - With "any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties."
  - Defines "foreign intelligence information"
- Adds "catch all" category for all other kinds of criminal investigative information

Section 204 – cont'd.

- DOJ supposed to create procedures for sharing GJ and T3 info. on U.S. Persons
- What do you do now?
  - Consult AUSA involved in GJ, T3
  - AUSA will arrange appropriate notice to Ct.
  - Can then disseminate, use in FISA process, etc.
- Current proposal to extend this to state officials

Section 206: Roving FISA

- Analogous to T3 language:
  - "actions of the target may have the effect of thwarting the identification of the specified person [on whom to serve the secondary order]"
  - FISC may now issue "generic" secondary order that can be used on new phone provider, landlord, ISP, etc.
- "Intent" requirement is less strict than T3; I.e., actions "may have the effect"

Section 206 Implementation

- OIPR developing standard language

b1
b7E

(S)

- Relations with FISC may affect this

Section 207: Duration

- All agent of a foreign power searches increase from 45 to 90 days.
- Non-U.S. Person "officer, employee, member" agents of a foreign power:
  - Initial ELSUR/search = 120 days
  - Renewal ELSUR/search = 1 year
- Should reduce overall number of FISA applications; speed up process

Section 208: Judges

- Number of FISC judges increases from seven to eleven
- Three must reside in Washington, D.C. area (up from one now)
- Will make emergency FISAs easier to schedule

Section 214: FISA Pen Registers

- Changes standard of FISA Pen/TT
  - Old = relevance + specific and articulable facts that target was AFP
  - New = just relevance to an ongoing investigation "to protect against international terrorism or clandestine intelligence activities"
  - First Amendment limitation

Section 214 - Implementation

- Means that FISA Pen/TT available in same circumstances as criminal case
- Pleadings are now being simplified, standardized
- Request to HQ need only state basis for relevance to investigation
- Note: same standard now applies to NSLs, Business records

Section 215: Business Records

- Same standard as Pen/TT
- Signed by FISA judge
- What you can get:
  - Old = records from common carriers, public accommodations, vehicle rentals, storage facilities
  - New = "any tangible things"

Section 215 - Implementation

- Use for things that don't fall within the categories of NSLs
- [redacted]
- Should be easy to get

b7E

Section 1003: Computer Trespasser language

- One of many computer crimes provisions in the Act
- Meant to obviate need for T3 in hacking cases.
- Section 1003 makes it apply to FISA as well
- Definitions are complex; call us if you think they apply

Sunset Provision

- December 31, 2005
- Applies to almost everything described above
- Areas to watch:
  - NSLs, Business Records, Pen/TT numbers and circumstances of use
  - FISA "primary purpose" issue
- Political circumstances will change

DID PC FOR FISA CHANGE?

- Target must be a foreign power or agent of a foreign power. Definitions remain the same.
- Facility at which ELSUR is to take place is used by a foreign power or agent of a foreign power

Structure of the Act

- National Security Stuff
  - Title II: "Enhanced Surveillance Procedures"
  - Title V: "Removing Obstacles to Investigating Terrorism"
- Other titles address money laundering, immigration, substantive criminal law

Title IIIs

- Section 201 of the USA Patriot Act added Material Support to Terrorism and other terrorism statutes as predicate offenses for Title IIIs.

Section 203: Sharing of criminal information with IC

- 203 amends Rule 6(e), Title III to allow sharing of Title III and GJ information:
  - With "any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties."
  - Defines "foreign intelligence information"
- Adds "catch all" category for all other kinds of criminal investigative information

Section 203 – cont'd.

- DOJ supposed to create procedures for sharing GJ and T3 info. on U.S. Persons
- What do you do now?
  - Consult AUSA involved in GJ, T3
  - AUSA will arrange appropriate notice to Ct.
  - Can then disseminate, use in FISA process, etc.
- Current proposal to extend this to state officials

Section 206: Roving FISA

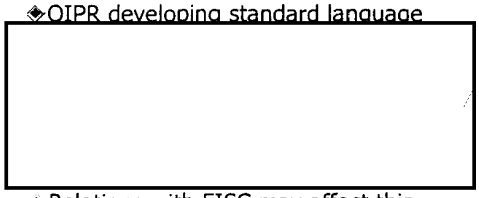
- Analogous to T3 language (18 U.S.C. 2518 (11)(b):
  - "actions of the target **may** have the effect of thwarting the identification of the specified person [on whom to serve the secondary order]"
  - FISC may now issue "generic" secondary order that can be used o[redacted]
- "Intent" requirement is different from T3; I.e., actions "may have the effect." In T3, the standard is "**could** have the effect"

(S) (S)

b1
b7E

Section 206 Implementation

- OIPR developing standard language



(S)

- Relations with FISC may affect this

Section 207: Duration

- **All** agents of a foreign power **searches** increase from 45 to 90 days.
- **Non-U.S. Person ELSUR** "officer, employee, member" agents of a foreign power (**not aiding and abetting**):
  - Initial ELSUR/search = 120 days
  - Renewal ELSUR/search = 1 year
  - **US Persons ELSURS still 90 days.**
  - Should reduce overall number of FISA applications; speed up process

b1

b7E

Section 208: Judges

- Number of FISC judges increases from seven to eleven
- Three must reside in Washington, D.C. area (up from one now)
- Will make emergency FISAs easier to schedule

Section 214: FISA Pen Registers

- Changes standard of FISA Pen/TT
  - Old = relevance + specific and articulable facts that target was AFP
  - New = just relevance to an ongoing investigation "to protect against international terrorism or clandestine intelligence activities"
  - First Amendment limitation--"is not conducted solely upon the basis of activities protected by the First Amendment"

Section 214 - Implementation

- Means that FISA Pen/TT available in same circumstances as criminal case
- Pleadings are now being simplified, standardized
- Request to HQ need only state basis for relevance to investigation
- Note: same standard now applies to NSLs, Business records

Section 215: Business Records

- Same standard as Pen/TT
- Signed by FISA judge
- What you can get:
  - Old = records from common carriers, public accommodations, vehicle rentals, storage facilities
  - New = "any tangible things" (Books, papers, records, documents, other items)

Section 215 - Implementation

- Use for things that don't fall within the categories of NSLs
- [redacted]
- Should be easy to get

Sections 218, 504: Purpose

- Section 218 requires that FISA certification say the foreign intelligence is a "significant purpose" of the FISA; old language said "the purpose" {which FISC took to mean "primary purpose."}
- Section 504 says it is OK for agents running FISAs to consult with criminal prosecutors (They may not direct a FISA.)

b7E

What does it mean?

- This is Congress and DOJ trying to fix the criminal/intelligence "wall" problems
- Issue here is how much can be fixed by statute, how much is a matter of Constitutional law

Section 223: Civil Liability

- Applies to unauthorized disclosure of FISA information
- Part of larger Congressional concern over abuse of broader surveillance authorities
- Provision (and others like it) watered down substantially
- Probably doesn't change much, since unauthorized disclosure already subject to heavy sanctions

Section 225: Immunity

- People [redacted] are immune from civil liability arising from compliance with FISA orders.
- Should be helpful in liaison with FISA order recipients and their lawyers

Section 505: NSLs

- Changes them to relevance standard
- Allows delegation to field

b7E

Section 905: Reporting to DCI

- Law enforcement now required to report foreign intelligence to DCI.
- AG will establish procedures on how to do this.
- Other provisions in statute for training of state and local officials to recognize, use FI.

Section 1003: Computer Trespasser language

- One of many computer crimes provisions in the Act
- Meant to obviate need for T3 in hacking cases.
- Section 1003 makes it apply to FISA as well
- Definitions are complex; call us if you think they apply

Sunset Provision

- December 31, 2005
- Applies to almost everything described above
- Areas to watch:
  - NSLs, Business Records, Pen/TT numbers and circumstances of use
  - FISA "primary purpose" issue
- Political circumstances will change

Intelligence Authorization Act for FY2002

- Signed December 28, 2001
- Technical fixes to USA PATRIOT Act
- Extends authorization period for emergency FISAs from 24 to 72 hours

Laundry List

- FISA Search Warrant Returns
- IOB Situation
- Investigations
- Training
- Revision of Minimization Rules
- Etc.

USA Patriot Act of 2001

[redacted]

National Security Law Branch
Office of the General Counsel

[redacted]

THE PATRIOT ACT 2001 National Security Provisions

b2
b6
b7C

Background of the USA PATRIOT Act

- Initial drafting began almost immediately after 9/11
- Incorporated some pending proposals, but mostly new proposals
- Most FBI proposals went into draft
- National Security, FISA provisions among the least controversial parts of the draft
- Two parts of note: Title II Enhanced Surveillance Procedures and Title V Removing Obstacles to Investigating Terrorism
- President signed on October 26, 2001

Amended FISA re: Significant Purpose

- Attempt to fix "wall" – promote sharing of criminal and foreign intelligence (FI) info
- **Section 218** – FI gathering as "significant purpose" replaces FI as "the purpose" of FISA Elsur and Phy. Search ("The purpose" language had been interpreted by FISC as "primary" purpose.) 18 USC 1804 (a)(7)(B), 1823 (a)(7)(B)
- Under FISA Court of Review, primary purpose can be criminal if it is a FI-related crime, but significant purpose must still be FI gathering.
- Primary purpose CANNOT be non-FI crime
- This provision will sunset December 31, 2005

Amended FISA re: Intell Consultation w/ Law Enforcement

- **Section 504** – federal officers running FISAs to acquire FI can consult with federal law enforcement (LE) officers to coordinate efforts to investigate or protect against attack, sabotage, IT, clandestine intell activities -- without undermining "significant" purpose. 50 USC 1806(k)(1)
- Removes fear that consulting with criminal prosecutors will negate FI "purpose" and prevent FISA.

Amended GJ/Title III re: Info Sharing of FI by LE

- Sharing of FI info from GJ or Title III wiretap w/ Intell officials
- **Section 203:** amended Fed. R. Crim. Proc. Rule 6(e) and Title III, 18 USC 2517(6), to allow sharing of Title III and GJ information involving foreign intell or counter intell with other federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent necessary to perform his duty.
- GJ-must notify court of dissemination
- AG Guidelines have been issued on GJ dissemination and can be found on ILU/OGC website

Amended Title III re: Definition of FI

- Added Definition of Foreign Intelligence to Title III, 18 USC 2510 (19), and GJ – Rule 6e(3)(C)(iv):
  - Information whether or not concerning a USP, that relates to the ability of the US to protect against
    - Actual or potential attack or other grave hostile acts of a foreign power or an AFP;
    - Sabotage or int'l terrorism by a foreign power or AFP; or
    - Clandestine intelligence activities by an intelligence service or network of a foreign power or by an AFP, or
  - Information whether or not concerning a USP, with respect to a foreign power or foreign territory that relates to
    - The national defense or security of the US; or
    - The conduct of the foreign affairs of the US.

- The provisions relating to Title III sharing (not GJ sharing) will sunset December 31, 2005

Created Catch-all Provision For Sharing of FI by LE

- **Section 203 catch-all:** "notwithstanding any other law," it is lawful for criminal investigators to share FI info obtained in course of a criminal investigation with any other federal law enforcement, intelligence, protective, immigration, national defense, or national security official.
- FI defined the same as under Title III and Fed. R. Crim. Proc. R. 6e (see previous slide)
- This provision will sunset December 31, 2005

Created Provision for Info Sharing with CIA

- **Section 905** – Law Enforcement must disclose FI acquired during course of criminal investigation to Director, CIA. 50 USC 403-5b.
- AG Guidelines have been issued on this section and can be found on the website of ILU/OGC

Amended FISA re: Roving FISA

(S)

- **Section 206:** Roving FISA authority [redacted] in order to circumvent surveillance – can get generic order and serve it on new service provider, even though not identified in order. 50 USC 1805(c)(2)(B)
- Requirement: "action of the target . . .may have the effect of thwarting the identification of the specified person [on whom to serve the order]"
- Analogous to Title III, 18 USC 2518(11) ("could have effect of thwarting interception from a specified facility"):

- This provision will sunset December 31, 2005

b1

Amended FISA re: Duration of Authority

- **Section 207:**
- All agent of a foreign power physical searches increase from 45 to 90 days. 50 USC 1824(d)(1)
- Non-USP "officer, employee, member" agents of a foreign power, per (101)(b)(1)(A) agent of foreign power):
  - Initial ELSUR/search = 120 days instead of 90 days
  - Renewal ELSUR/search = 1 year instead of 90 days

This provision will sunset December 31, 2005

Amended FISA re: Number of FISC Judges

- **Section 208:** Number of FISC judges increases from seven to eleven
- Three must reside in Washington, D.C. area (up from one)
- Makes emergency FISAs easier to schedule
- Practical effect is that Court sits more than scheduled Friday hearing

Amended FISA re: Pen Registers

- **Section 214**: Changed standard of FISA Pen Register/Trap and Trace court order. 50 USC 1842(c)2.
- Before - relevance + specific and articulable facts that target was agent of foreign power
- Now - just relevance to an ongoing investigation "to protect against international terrorism or clandestine intelligence activities" or info likely to be obtained is FI not concerning USP, and investigation of USP is not based solely on First Amendment activities

b1

- This provision will sunset December 31, 2005 (S)

FISA Pen Register – Cont.

(S)

b1
b5

Amended Provision of FISA for Business Records

- **Section 215**: Changed standard to same relevance standard as Pen Register/TT court order and National Security Letters. 50 USC 1861 (a)(1).
- Provision enacted in 1998 to provide for records from common carriers, public accommodations, vehicle rentals, storage facilities – based on relevance and specific and articulable facts that records related to agent of foreign power
- Now - "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities" provided investigation of U.S. person not based solely on First Amendment rights

Business Records – cont.

Statute says Director (not AG, like other parts of FISA statute) may apply for order – Director has delegated authority to EAD, ADs, DADs, OGC etc., at HDQR level

- NSLB and OIPR have agreed to form, awaiting AG approval.
- Business records form available for field to fill out and submit to headquarters and NSLB (attn:
-
- Likely that application to FISC and order will be classified (S)
- This provision will sunset December 31, 2005

b1
b6
b7C

Business Records – cont.

Amended Provisions re: National Security Letters

- Three NSLs – administrative subpoenas that allow the FBI to obtain
  - phone and email communication records from telephone companies and internet service providers (Electronic Communications Privacy Act) (18 USC 2709)
  - financial institution records (Right to Fin. Privacy Act) (12 USC 3414(a)(5)(A))
  - credit bureau info – identity of financial institutions and consumer identifying information (Fair Credit Reporting Act) (15 USC 1681u (a), (b)) (full report if ct. order)

b5

~~SECRET~~

Amended Provision- Title III expectation of privacy

- Adds provision, Title IIII, 18 USC 2510(21), defining computer trespasser as "person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communications transmitted to, through, or from the protected computer.
- Thus, allows for electronic surveillance of computer trespasser without Title III or FISA surveillance.

Amended Provision - Computer Trespasser Interceptions w/o Title III authority

- **Section 217**: Amended 18 USC Section 2511 to provide for four requirements allowing surveillance of person defined as "computer trespasser" of "protected computer" (as defined in 18 USC 1030) without Title III or FISA authority:
  - Owner of protected computer authorizes interception,
  - Government is engaged in lawful investigation,
  - Government has reasonable grounds to believe that the contents of communication will be relevant to the investigation, and
  - Interception does not acquire communications other than those of the computer trespasser

This provision will sunset on December 31, 2005.

Amended Provision - Assets of Terrorists Organizations Subject to Civil Forfeiture

- **Section 806** : Amends 18 USC 981(a)(1), to include (G) which makes the following property subject to civil forfeiture: All assets, foreign or domestic:
  - of any individual, entity or organization engage in planning or perpetrating any act of domestic or international terrorism (defined in 2331) against the U.S., citizens or residents of the U.S. or their property, and all assets, foreign or domestic, affording any person a source of influence over any such entity or organization;
  - acquired or maintained by any person with the intent and for the purpose of supporting, planning, conducting, or concealing an act of domestic or international terrorism (defined in 2331) against the U.S., citizens or residents of the U.S., or their property; or
  - derived from, involved in, or used or intended to be used to commit any act of domestic or international terrorism (defined in 2331) against the U. S., citizens or residents of the U.S., or their property.

Expanded Voluntary Disclosure by Communications Providers

- **Section 212** – Added to 18 USC 2702(b) grounds for provider to voluntarily disclose contents of customer communications or records, to include "if provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure."
- Added 18 USC 2702 (c), providing for voluntary disclosure, excluding contents, if emergency, as defined above, or if "necessarily incident to the rendition of the service or to the protection of the rights or property of the provider."
- This provision will sunset December 31, 2005

~~SECRET~~

Amended ECPA – Expanded Scope of Subpoenas for Electronic Surveillance

- Pre-Patriot Act - Use of subpoena to compel limited subscriber information (name, address, length of service, means of payment), however, could not obtain credit card number or other payment methods. Also ECPA was tech-specific, i.e. telephone = "local and long distance toll billing records" but did not include parallel terms for computer communications.
- **Section 210** – Amended ECPA, 18 USC 2703(c) to expand list of records government can obtain with a subpoena, for computers, to include "records of session times and durations" as well as "any temporarily assigned network address." Also use of a subpoena to obtain "means and source of payment" including credit card or bank account number , for both telephone and computer services.

Amended ECPA – Search Warrants for Contents of Stored Voice-Mail

- Pre Patriot Act - Search Warrant required for contents of stored electronic communications (e-mail) pursuant to ECPA (18 USC 2703) and Title III required for contents of stored wire communications (voice-mail) pursuant to Title III (18 USC 2510).
- **Section 209** - Amends ECPA and Title III, to allow for the use of search warrants pursuant to ECPA (18 USC 2703) to obtain contents of "wire or electronic communications" rather than simply "electronic" communications."
- This provision will sunset on December 31, 2005

~~SECRET~~

Amended ECPA - Single Jurisdiction Warrants for Stored Voice Mail/E-Mail Contents

- **Section 220**: Amended ECPA, Section 2703(a) to allow search warrant for contents of stored voice mail and e-mail to be issued by "court with jurisdiction over the offense under investigation," i.e., nationwide jurisdiction - one court can issue all warrants involved in a case even if service provider or target is located outside the issuing district.
- This provision will sunset on December 31, 2005

Amended Fed. R. Cr. Proc. R. 41- Search Warrants - Single Jurisdiction in DT and IT cases

- **Section 219**: Amended Rule 41(a) Federal Rules of Criminal Procedure to provide that, in Domestic and International Terrorism investigations, a search warrant issued by court "in any district in which activities related to the terrorism activities have occurred for a search of property or persons located within or outside of the district."

Created Provision - Delayed Notice on Search Warrants

- **Section 213**: Adds provision to 18 USC 3103a creating a uniform statutory standard (as 18 USC 2705 already provides for delayed notice when seeking stored communications through court order or subpoena) authorizing courts to delay the required notice of the execution of any warrant or court order if "reasonable cause" to believe that providing notice may have an adverse result as defined by 18 USC 2705 (including endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation).
- Warrant must prohibit seizure of tangible property, wire or electronic communication, or, except as expressly provided in 18 USC 2705, stored wire or electronic information.
- So-called sneak and peek searches
- Must give notice within reasonable period, or extended for good cause by Court

Clarified PR/TT To Include Computer Information

- Pre-Patriot Act - Criminal PR/TT statute (1986) provided for the prospective collection of non-content traffic information from telephone line and did not envision communication over computers.
- **Section 216**: Updated the PR/TT statute:
  - Clarified that statute applies to computer communications – applies to telephone line "or other facility, " 18 USC 3123.
  - Facility also includes cellular telephone or a specific cell-phone identified by an ESN.
  - Defined "Pen Register," 18 USC 3127, to include computer terms: device which records or decodes "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, " (e.g. IP address, port numbers, "to" and "from" on email header; not subject line or content).

~~SECRET~~

Amended PR/TT Single Jurisdiction Court Order

- **Section 216** – PR/TT order issued by "court of competent jurisdiction, " 18 USC 3122, defined as court "having jurisdiction over the offense being investigated," (18 USC 3127(2)).
- Nationwide jurisdiction – similar to ECPA stored wire and voice mail search warrants - one court can issue all warrants involved in a case even if service provider or target is located outside the issuing district.

Amended PR/TT Re: Reporting

- **Section 216**: Requires law enforcement to file a special report ex parte and under seal with the Court within 30 days after termination of PR/TT order whenever law enforcement uses its own monitoring device, 18 USC 3123(3).
  - Report must contained identity of officer who installed device, date and time device installed, configuration of device, information collected from the device

In Congress

- Senate passed version close to the Administration's draft (USA Act)
- House version substantially different, but substituted at last minute for something like the Senate version
- House insisted on "sunset" provision
- House passes PATRIOT Act
- Conference, then USA PATRIOT Act passed
- President signed on October 26, 2001

Structure of the Act

- National Security Stuff
  - Title II: "Enhanced Surveillance Procedures"
  - Title V: "Removing Obstacles to Investigating Terrorism"
- Other titles address money laundering, immigration, substantive criminal law
- Other stuff

Section 204: Sharing of criminal information with IC

- 204 amends Rule 6(e), Title III to allow sharing of Title III and GJ information:
  - With "any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties."
  - Defines "foreign intelligence information"
- Adds "catch all" category for all other kinds of criminal investigative information

Section 204 – cont'd.

- DOJ supposed to create procedures for sharing GJ and T3 info. on U.S. Persons
- What do you do now?
  - Consult AUSA involved in GJ, T3
  - AUSA will arrange appropriate notice to Ct.
  - Can then disseminate [redacted]
- Current proposal to extend this to state officials (S)

b1

Section 206: Roving FISA

- Analogous to T3 language:
  - "actions of the target may have the effect of thwarting the identification of the specified person [on whom to serve the secondary order]"
  - FISC may now issue "generic" secondary order [redacted] (S)
- "Intent" requirement is less strict than T3; I.e., actions "may have the effect"

b1

Section 206 Implementation

- OIPR developing standard language [redacted] (S)
- Relations with FISC may affect this

b1
b7E

Section 207: Duration

- All agent of a foreign power searches increase from 45 to 90 days.
- Non-U.S. Person "officer, employee, member" agents of a foreign power:
  - Initial ELSUR/search = 120 days
  - Renewal ELSUR/search = 1 year
- Should reduce overall number of FISA applications; speed up process

Section 208: Judges

- Number of FISC judges increases from seven to eleven
- Three must reside in Washington, D.C. area (up from one now)
- Will make emergency FISAs easier to schedule

Section 214: FISA Pen Registers

- Changes standard of FISA Pen/TT
  - Old = relevance + specific and articulable facts that target was AFP
  - New = just relevance to an ongoing investigation "to protect against international terrorism or clandestine intelligence activities"
  - First Amendment limitation

Section 214 - Implementation

- Means that FISA Pen/TT available in same circumstances as criminal case
- Pleadings are now being simplified, standardized
- Request to HQ need only state basis for relevance to investigation
- Note: same standard now applies to NSLs, Business records

Section 215: Business Records

- Same standard as Pen/TT
- Signed by FISA judge
- What you can get:
  - Old = records from common carriers, public accommodations, vehicle rentals, storage facilities
  - New = "any tangible things"

Section 215 - Implementation

- Use for things that don't fall within the categories of NSLs

b7E

-
- Should be easy to get

Sections 218, 504: Purpose

- Section 218 requires that FISA certification say the foreign intelligence is a "significant purpose" of the FISA; old language said "the purpose" {which FISC took to mean "primary purpose."}
- Section 504 says it is OK for agents running FISAs to consult with criminal prosecutors

What does it mean?

- This is Congress and DOJ trying to fix the criminal/intelligence "wall" problems
- Issue here is how much can be fixed by statute, how much is a matter of Constitutional law
- Stay tuned for this afternoon's discussion

Section 223: Civil Liability

- Applies to unauthorized disclosure of FISA information
- Part of larger Congressional concern over abuse of broader surveillance authorities
- Provision (and others like it) watered down substantially
- Probably doesn't change much, since unauthorized disclosure already subject to heavy sanctions

Section 225: Immunity

- People [redacted] are immune from civil liability arising from compliance with FISA orders.
- Should be helpful in liaison with FISA order recipients and their lawyers

b7E

Section 505: NSLs

- Changes them to relevance standard
- Allows delegation to field
- Much more to come this afternoon

Section 905: Reporting to DCI

- Law enforcement now required to report foreign intelligence to DCI.
- AG will establish procedures on how to do this.
- Other provisions in statute for training of state and local officials to recognize, use FI.
- Real story?

Section 1003: Computer Trespasser language

- One of many computer crimes provisions in the Act
- Meant to obviate need for T3 in hacking cases.
- Section 1003 makes it apply to FISA as well
- Definitions are complex; call us if you think they apply

Sunset Provision

- December 31, 2005
- Applies to almost everything described above
- Areas to watch:
  - NSLs, Business Records, Pen/TT numbers and circumstances of use
  - FISA "primary purpose" issue
- Political circumstances will change

Intelligence Authorization Act for FY2002

- Signed December 28, 2001
- Technical fixes to USA PATRIOT Act
- Extends authorization period for emergency FISAs from 24 to 72 hours

Laundry List

- FISA Search Warrant Returns
- IOB Situation
- Investigations
- Training
- Revision of Minimization Rules
- Etc.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 22
Page 7 ~ Referral/Direct
Page 42 ~ Duplicate
Page 43 ~ Duplicate
Page 44 ~ Duplicate
Page 45 ~ Duplicate
Page 46 ~ Duplicate
Page 47 ~ Duplicate
Page 48 ~ Duplicate
Page 49 ~ Duplicate
Page 50 ~ Duplicate
Page 51 ~ Duplicate
Page 52 ~ Duplicate
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 55 ~ Duplicate
Page 56 ~ Duplicate
Page 57 ~ Duplicate
Page 72 ~ Duplicate
Page 73 ~ Duplicate
Page 74 ~ Duplicate
Page 75 ~ Duplicate
Page 76 ~ Duplicate Miranda e-mail, FDPS pg. 12

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE **Date:** 11/28/2001

To: All Field Offices **Attn:** ADIC;
SAC;
CDC
FCI/IT Supervisors

Counterterrorism AD Watson;
DADs;
Section Chiefs

National Security AD Gallagher;
DADs;
Section Chiefs

From: General Counsel
National Security Law Unit, Room [redacted]
Contact: [redacted]

Approved By: Mueller Robert S III
Pickard Thomas J
Parkinson Larry R
Bowman M E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-09-2005 BY 65179 DMH/ELH 05-cv-0845

b2
b6
b7C

Drafted By: [redacted] jw
Jr:jrl

Case ID #: 66F-HQ-A1255972

Title: NATIONAL SECURITY LETTER MATTERS

Synopsis: Provides guidance on the preparation, approval, and service of National Security Letters (NSLs).

Reference: 66F-HQ-A1255972 Serial 15

Enclosure(s): [redacted]

b2
b7E

14) FCRA NSL Checklist

Details: In the referenced communication, dated 11/09/2001, the Director of the FBI delegated the authority to certify NSLs to the following officials: (1) the Deputy Director; (2) The Assistant Directors (ADs) and all Deputy Assistant Directors (DADs) of the Counterterrorism Division (CTD) and the National Security Division (NSD); (3) the General Counsel and the Deputy General Counsel for National Security Affairs (DGC), Office of the General Counsel (OGC); (4) the Assistant Director in Charge (ADIC), and all Special Agents in Charge (SACs), of the New York, Washington, D.C., and Los Angeles field divisions; and (5) the SACs in all other field divisions. The purpose of this electronic communication is to provide comprehensive guidance on the preparation, approval, and service of NSLs.

1. Introduction to National Security Letters

NSLs are administrative subpoenas that can be used to obtain several types of records. There are three types of NSLs. First, pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, the FBI can issue NSLs for: (1) telephone subscriber information (limited to name, address, and length of service); (2) telephone local and long distance toll billing records; and (3) electronic communication transactional records. Second, pursuant to the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5), the FBI can issue NSLs to obtain financial records from banks and other financial institutions. Finally, pursuant to the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u, the FBI can issue NSLs to obtain consumer identifying information and the identity of financial institutions from credit bureaus.

NSLs are tools available in investigations conducted under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). The FCIG currently provide that an NSL can be issued during the course of a full international terrorism or foreign counterintelligence investigation. **NSLs cannot be used in criminal investigations unrelated to international terrorism or clandestine intelligence activities.**

b2
b7E

b2
b7E

2. General Policy on the Use of NSL Authority

NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information. However, they must be used judiciously. The USA PATRIOT Act greatly broadened the FBI's authority to gather this information. However, the provisions of the Act relating to NSLs are subject to a "sunset" provision that calls for the expiration of those provisions in four years. In deciding whether or not to re-authorize the broadened authority, Congress certainly will examine the manner in which the FBI exercised it. Executive Order 12333 and the FCIG require that the FBI accomplish its investigations through the "least intrusive" means. Supervisors should keep this in mind when deciding whether or not a particular use of NSL authority is appropriate. The greater availability of NSLs does not mean that they should be used in every case.

In addition, the removal of any requirement for FBIHQ coordination in the issuing of NSLs creates the possibility of duplicate requests for the same information by different field offices. Field offices must take steps to avoid this. In particular, the field should check FBI databases (ACS, Telephone Application, etc.) and open sources to see if the information sought has already been obtained by the FBI or whether it is publically available. This is particularly important when considering issuing NSLs for telephone or electronic communications data under the Electronic Communications Privacy Act (ECPA). Unlike the criminal authorities in ECPA, the NSL authority does not require the government to reimburse carriers or Internet Service Providers (ISPs) for the cost of producing the requested information. A dramatic increase in duplicate NSLs will only augment existing pressure to require governmental reimbursement.

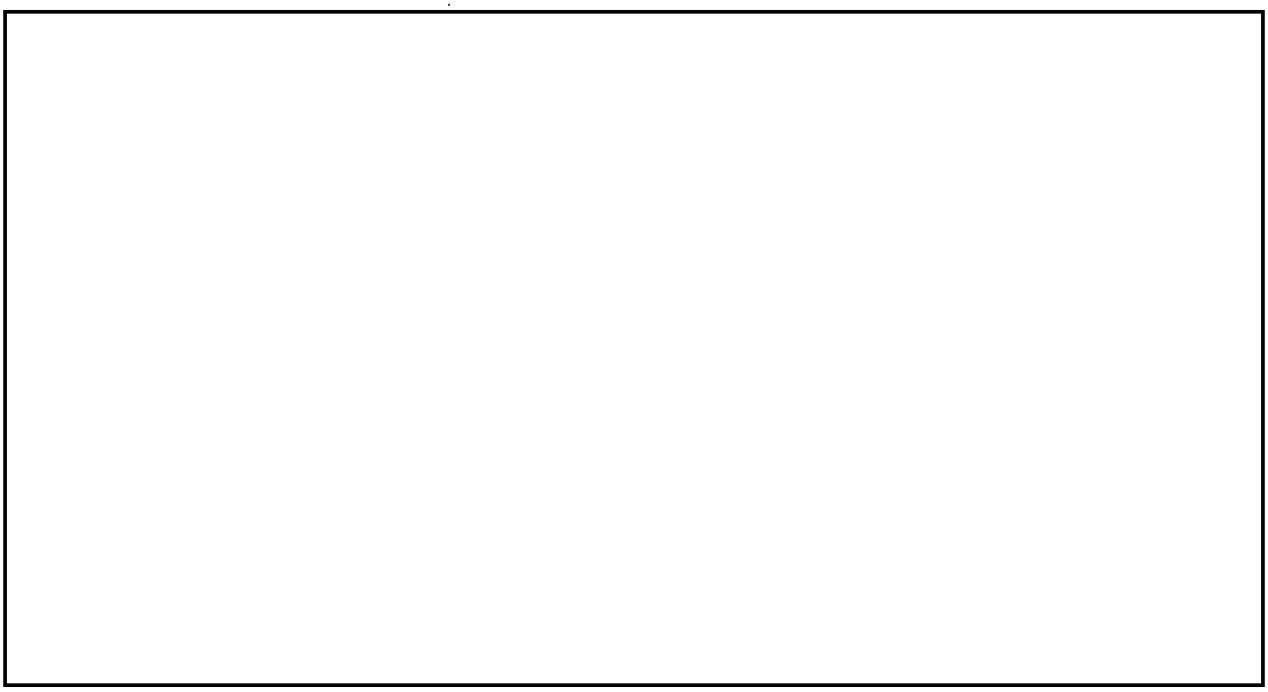
Individual field offices have the responsibility for establishing and enforcing an appropriate review and approval process for the use of NSL authorities.

3. The Mechanics of Producing NSLs

For all types of NSLs, the issuing office needs to prepare two documents: (1) the NSL itself; and (2) an EC approving the NSL and documenting the predication. Model NSLs and ECs for all variations of the three types of NSLs are included as attachments to this communication. These materials will also be placed on the [redacted] Once the initial implementation of these new authorities is accomplished, NSLU will work to develop a macro or form to further streamline the NSL process. b2 b7E

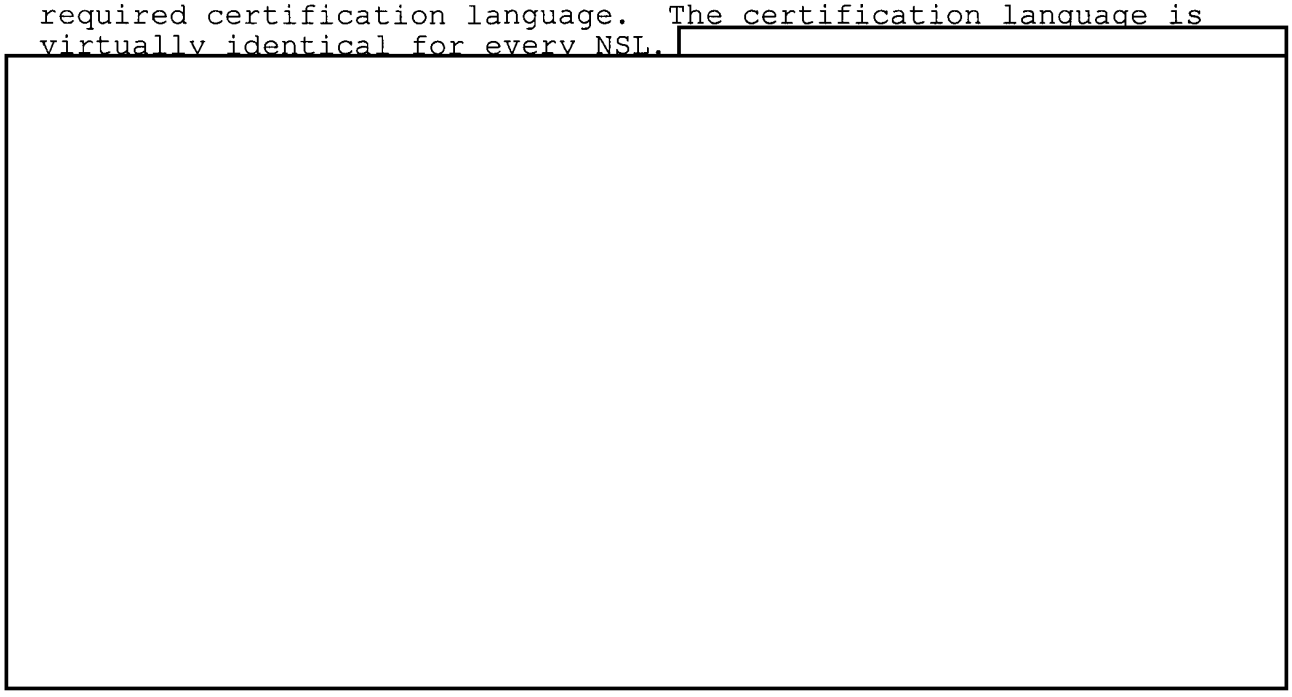
A. The NSL

[redacted] b2 b7E



b2
b7E

The second paragraph of every NSL contains the statutorily required certification language. The certification language is virtually identical for every NSL.



b2
b7E

The model NSLs for financial records and electronic communication transactional records each have a separate attachment. These attachments provide examples of information

which the company might consider to be financial or electronic communication transactional records.

Finally, the NSL is an unclassified document because it does not detail the specific relevance of the requested records to an authorized FBI investigation. There is no need to classify the NSL when attaching it to the cover EC.

B. The Cover EC

[redacted]

b2
b7E

1) Field Descriptors

[redacted]

b2
b7E

[redacted] b2 b7E

2) Predication and Relevance

The USA PATRIOT Act has greatly simplified the NSL process. The FBI official authorizing the issuance of an NSL is no longer required to certify that there are specific and articulable facts giving reason to believe that the information sought pertains to a foreign power, or an agent of a foreign power. NSLs may now be issued upon a certification of relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

[redacted] b2 b7E

The relevance requirement ties the requested records to the appropriate [redacted] b2 b7E

[redacted] b2 b7E

3) Approval

The second paragraph in the "Details" section and the "Approved By" descriptor field of the EC should reflect the level of the official approving the issuance of the EC and signing the NSL's certification. Prior to certification, every NSL and cover EC issued by the field division should be reviewed by the squad supervisor, the Office of the Chief Division Counsel, and the ASAC. Lawyers reviewing NSL packages should use the checklists provided with this communication to ensure legal sufficiency. The last step in the approval process occurs when the certifying official (Deputy Director, ADs, General Counsel, ADICs, DADs, DGC, or SACs) personally signs the NSL and initials the EC. Certifying officials may not further delegate signature authority.

4) Reporting Requirements

NSLU will continue to prepare the mandatory reports to Congress required for each NSL type. To ensure that NSLU receives sufficient information to prepare these reports, it is critical that the person preparing the NSL package follow the NSL and EC models very carefully. The second lead in every model EC requests NSLU to "record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs." NSLU will be able to compile the reporting data provided that the cover EC includes [redacted] being requested in the NSL. Once NSLU has entered this reporting data into its NSL database, it will clear the lead set in the cover EC. b2 b7E

5) Transmittal

[redacted] b2 b7E

[redacted] b2 b7E

4. NSL Preparation Assistance

Some field divisions may, for a variety of reasons, opt not to exercise their delegated authority to issue NSLs. Other field divisions may exceed their capacity to issue NSLs and seek assistance in handling the overflow. NSLU will continue to process any NSL request that it receives. Field divisions should send their requests directly to NSLU, with information copies to the FBIHQ substantive unit. Such requests must contain all the information identified in this communication as necessary to prepare the NSL package. NSLU anticipates that it will be able to process such requests within one to three business days.

Any questions regarding this communication may be directed to [redacted] NSLU, OGC, at [redacted] b6 b7C

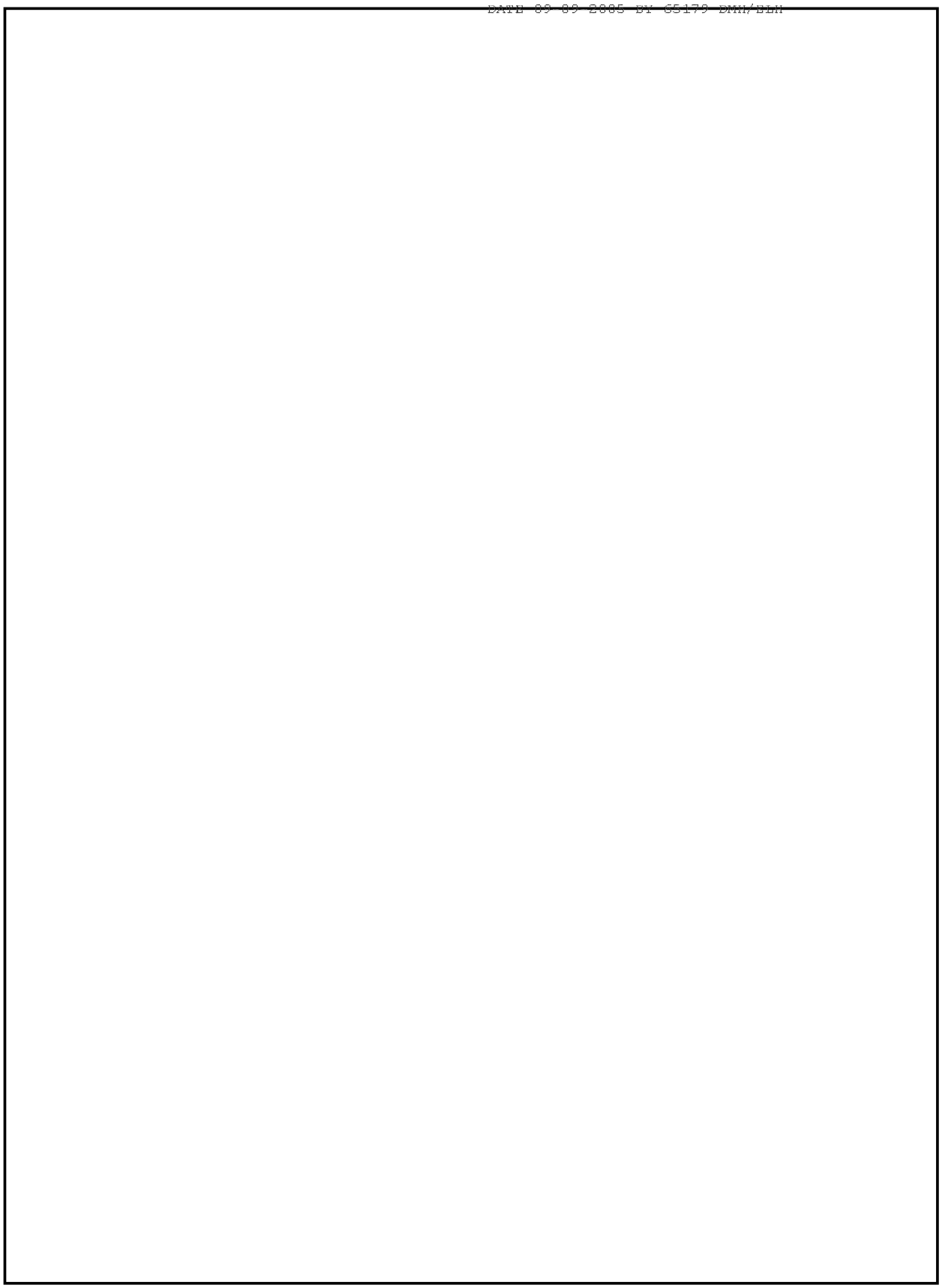
LEAD(s):

Set Lead 1: (Adm)

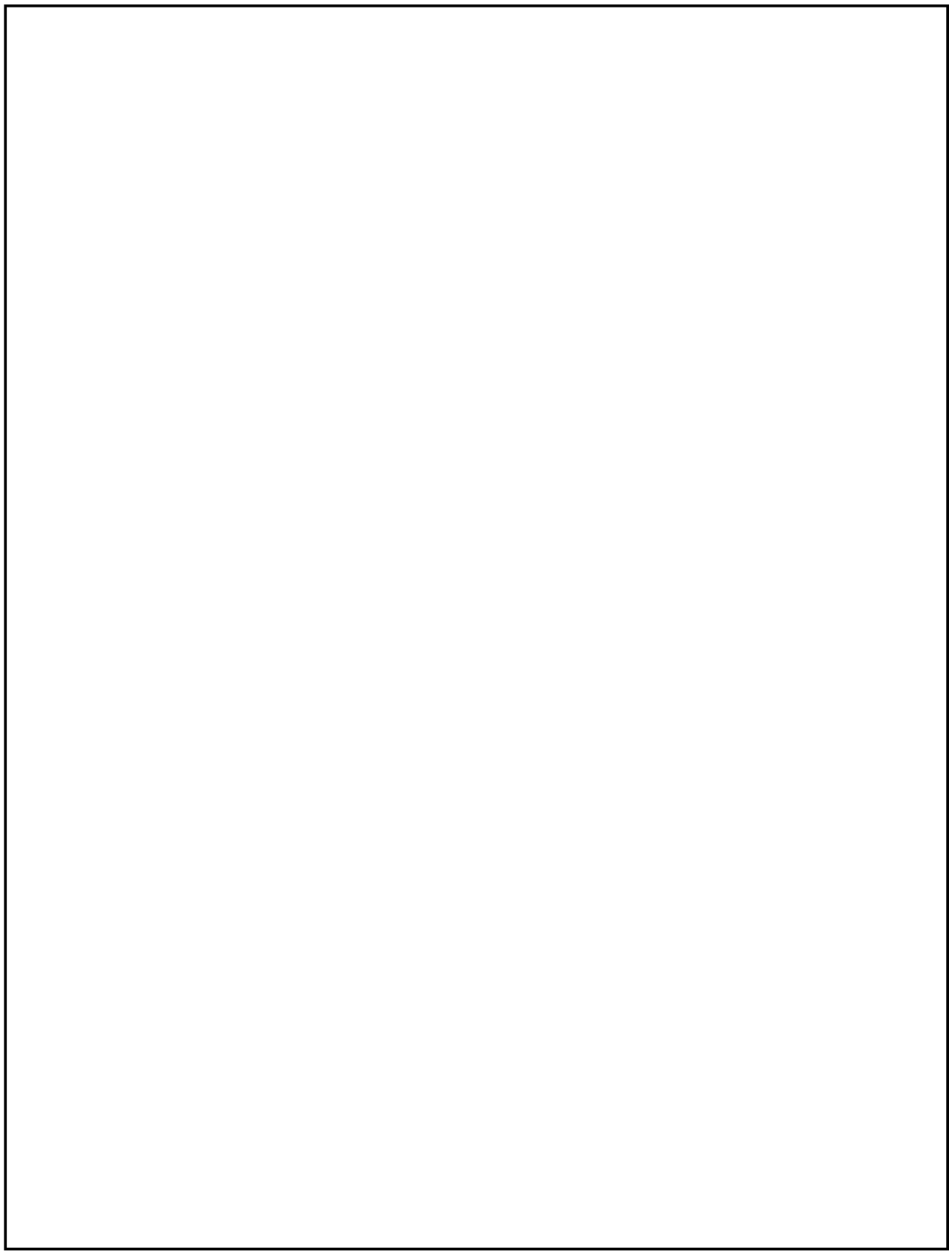
ALL RECEIVING OFFICES

Distribute to all supervisory personnel involved in the National Security Letter process.

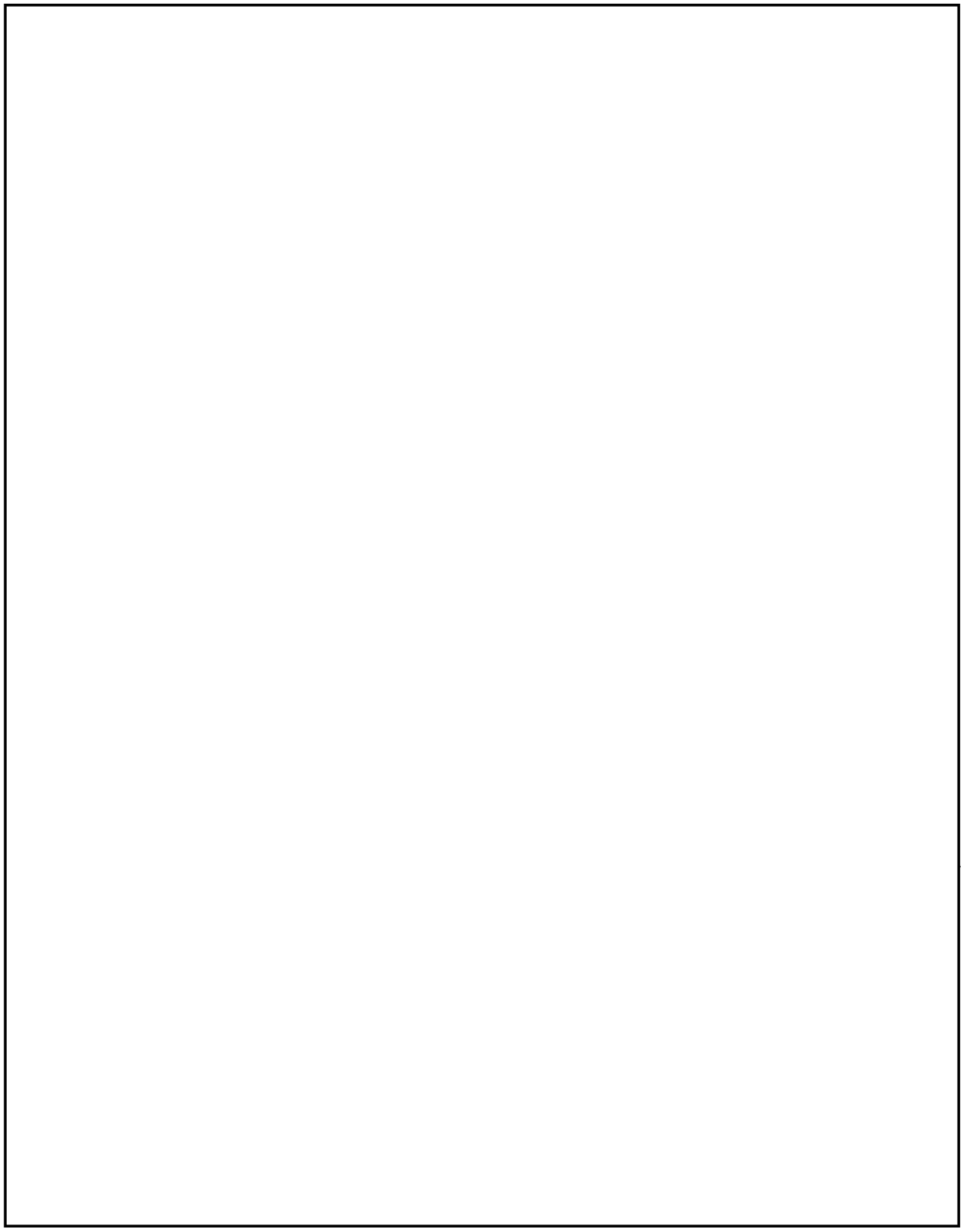
♦♦



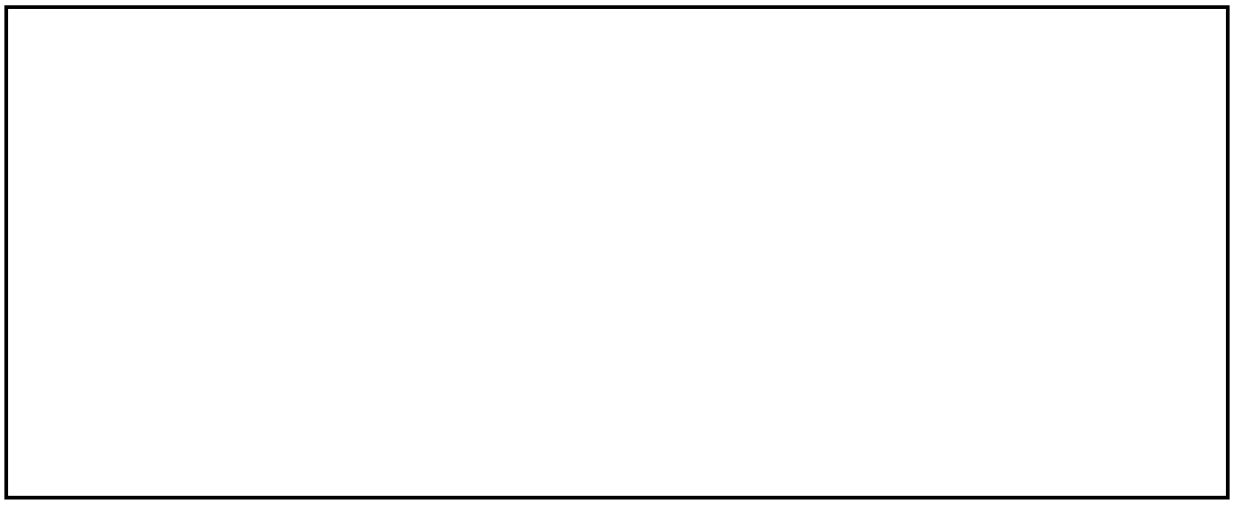
b5



b5



b5



b5

(Draft responses to Senate Judiciary QFRs, 07/14/2004)

QUESTIONS FOR 10/23/03 INTELLIGENCE COMMITTEE HEARING ON THE USA PATRIOT ACT

b5

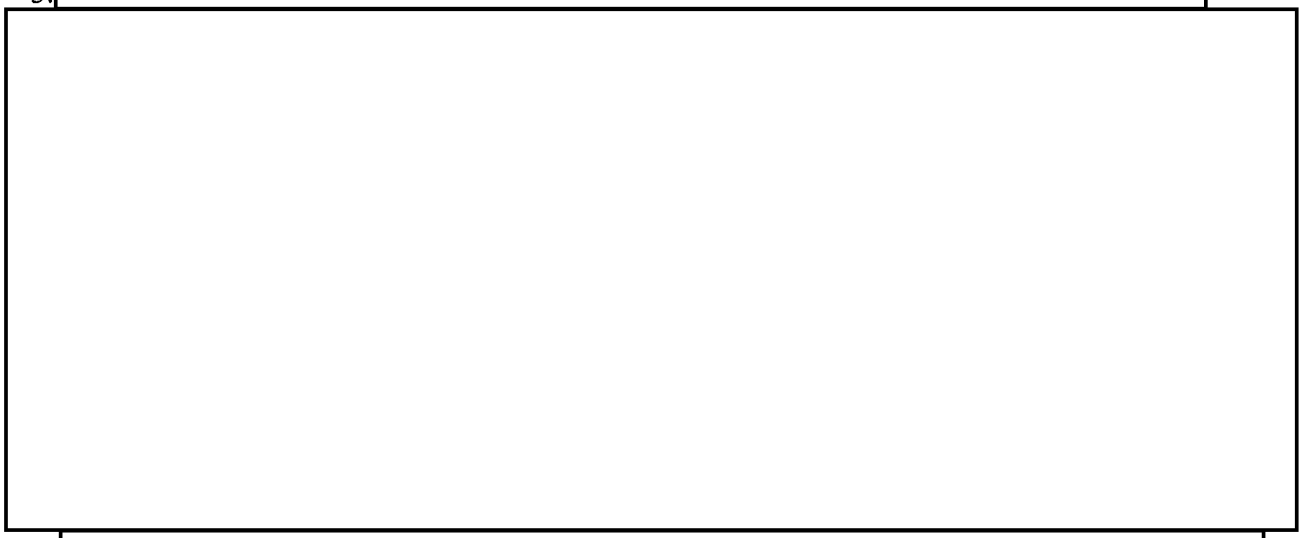
b6

b7C

b5

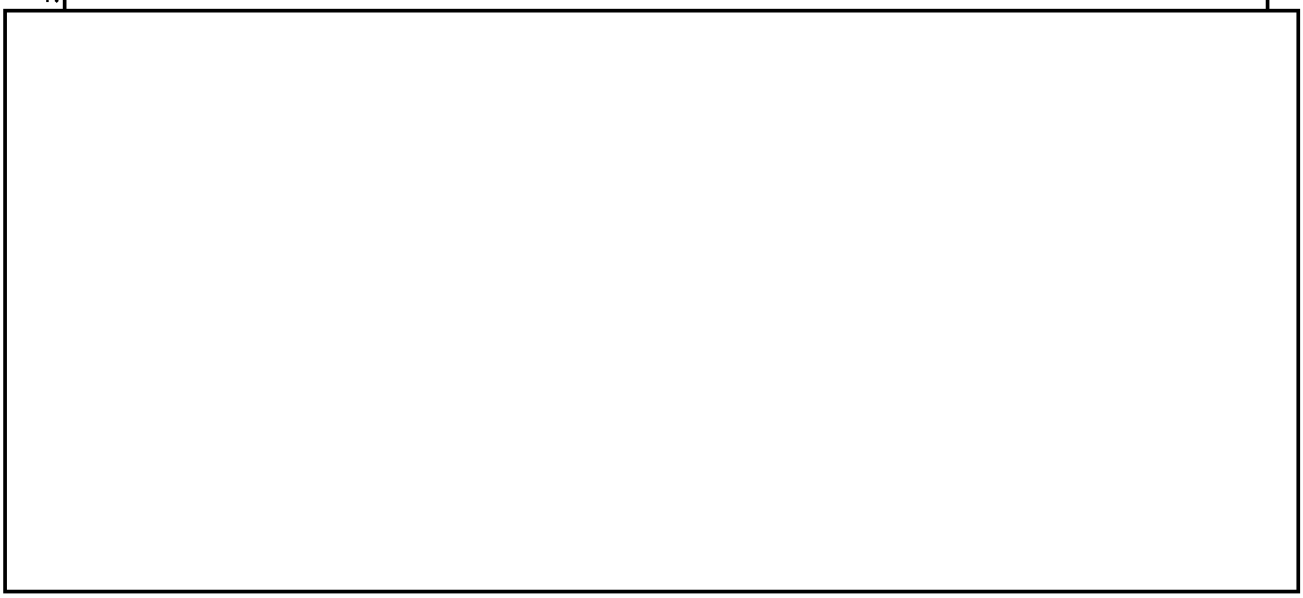
b5

3.

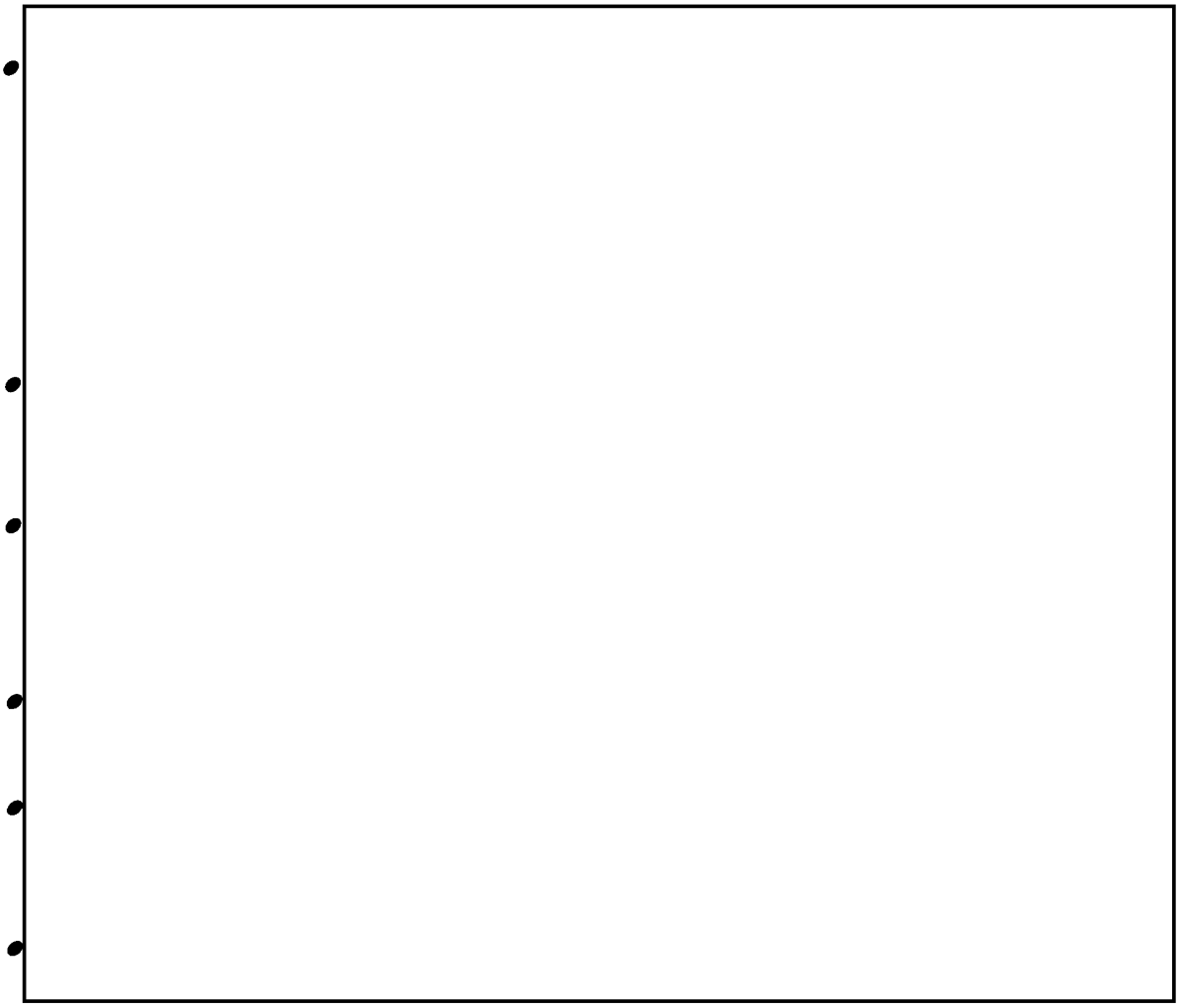


b5

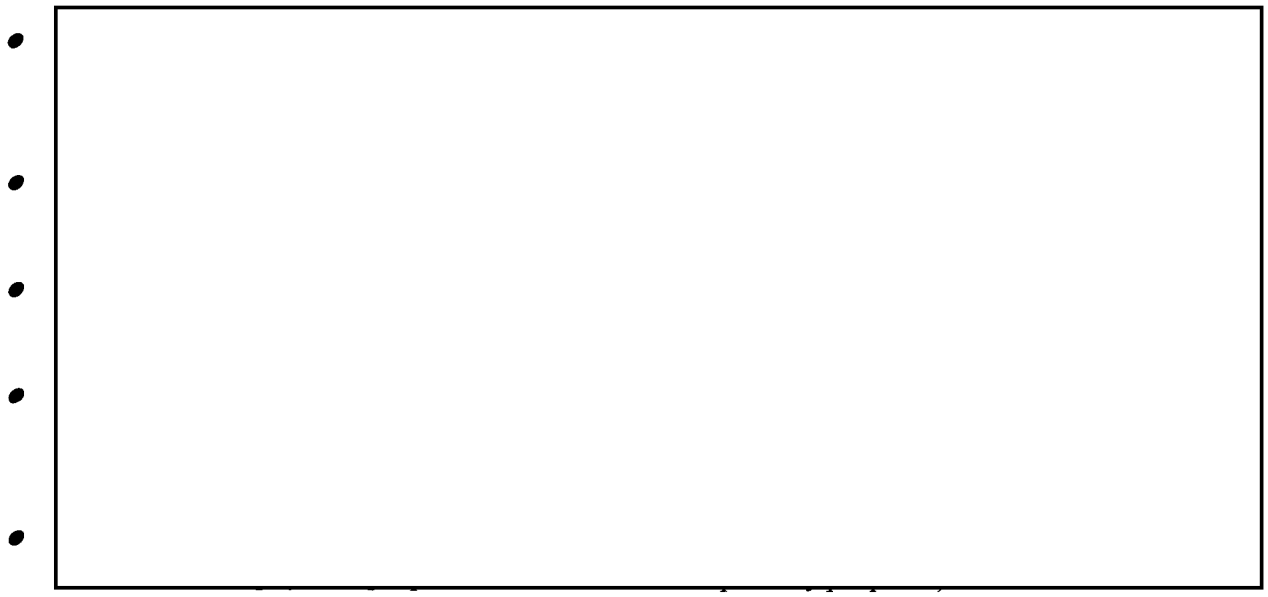
4.



b5



b5



b2
b7E
b5

- [redacted]
- [redacted]

b5

5. [redacted]

[redacted]

b5

- [redacted]

b5

- [redacted]
- [redacted]

- [redacted]

b5
b2
b7E

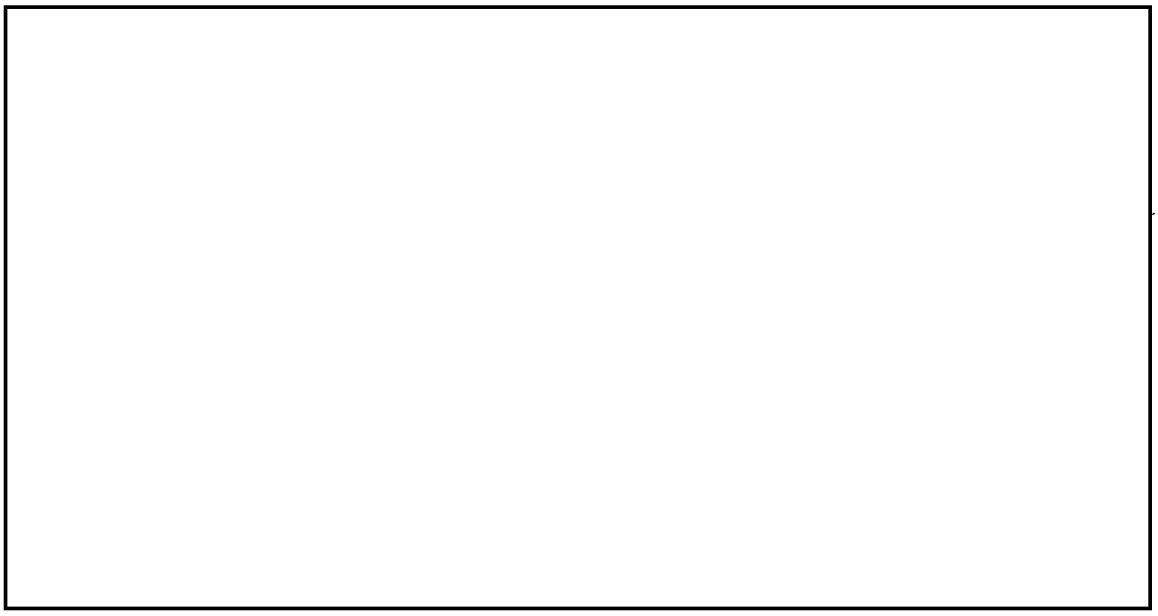
6. [redacted]

b5

- [redacted]
- [redacted]
- [redacted]

b5

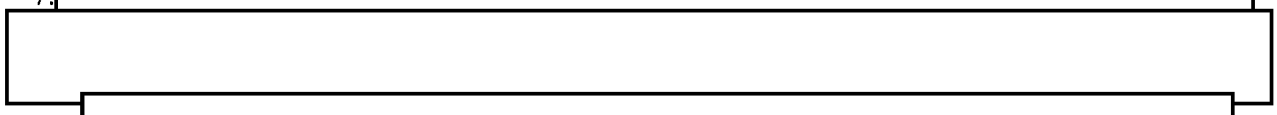
b5



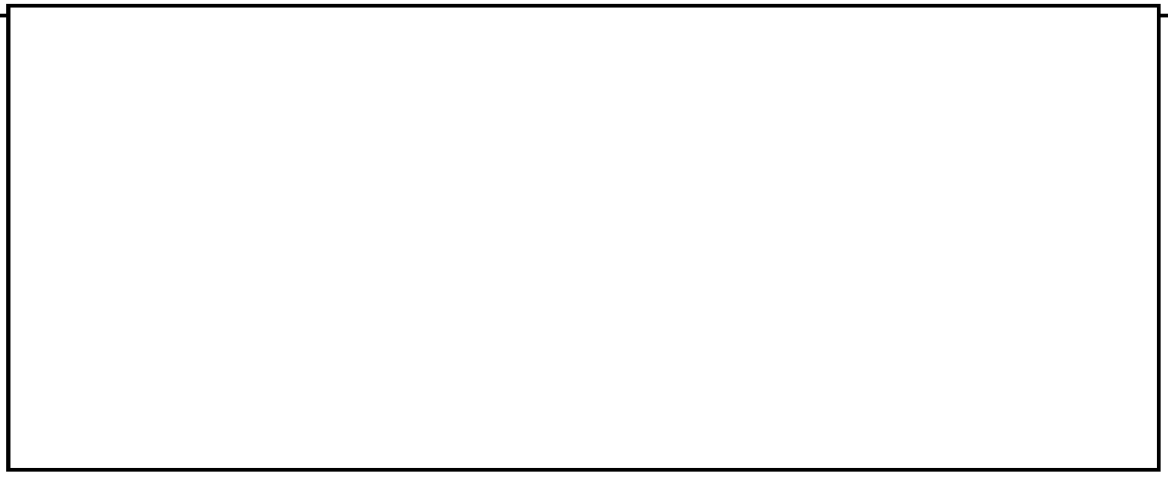
b5

- [redacted]

7. [redacted]



- [redacted]



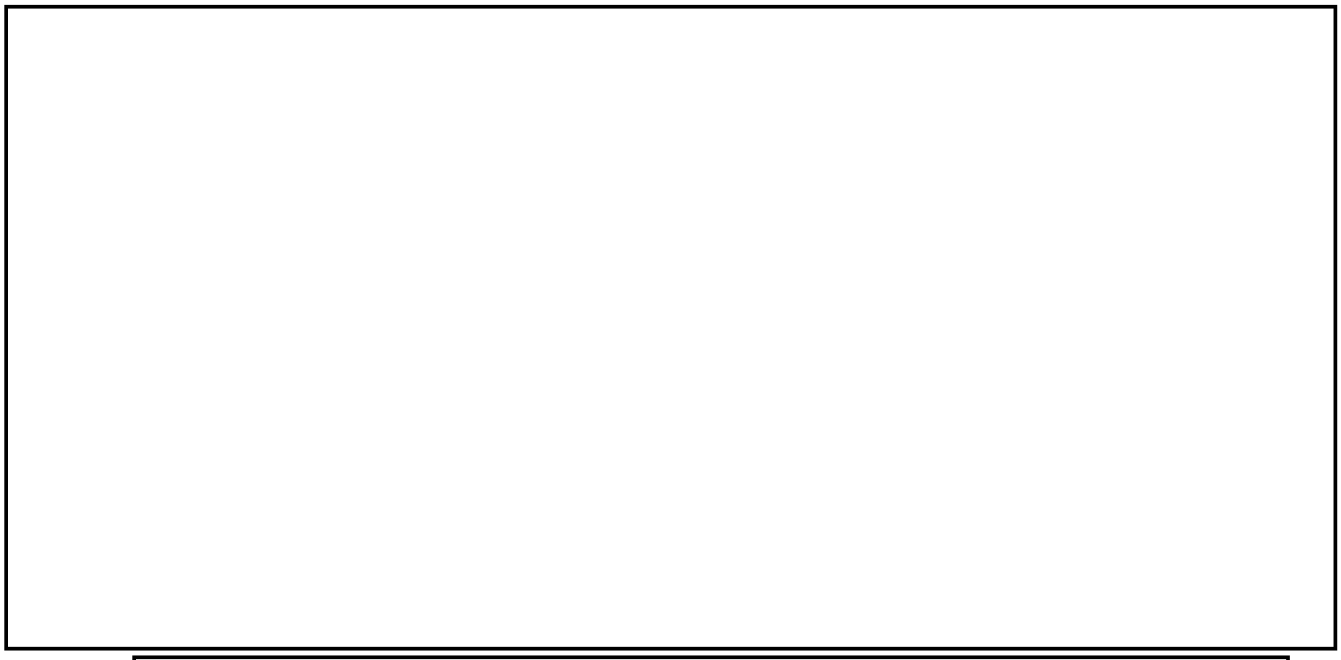
b5

- [redacted]

8. [redacted]

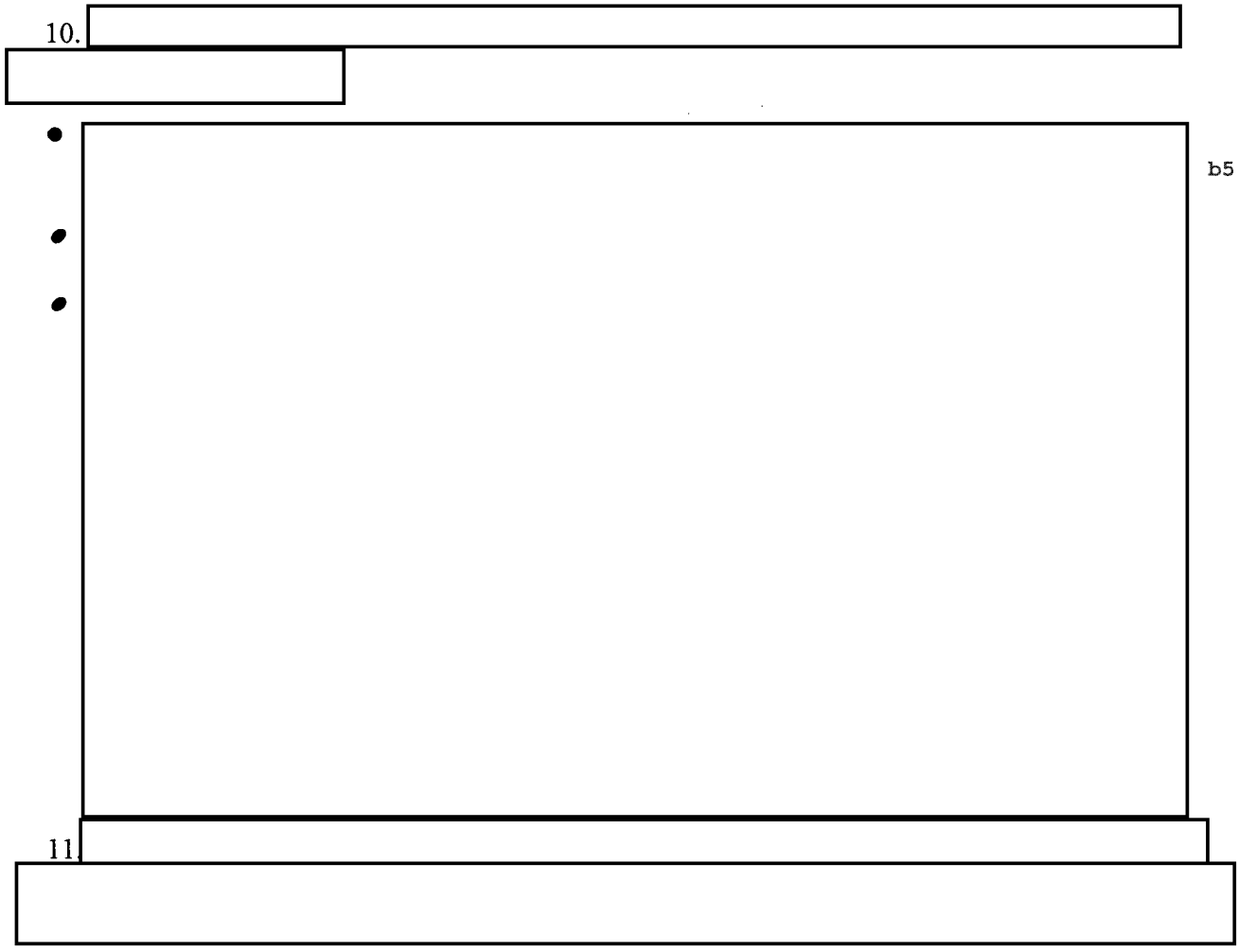
b5

9. [redacted]



b5

10.



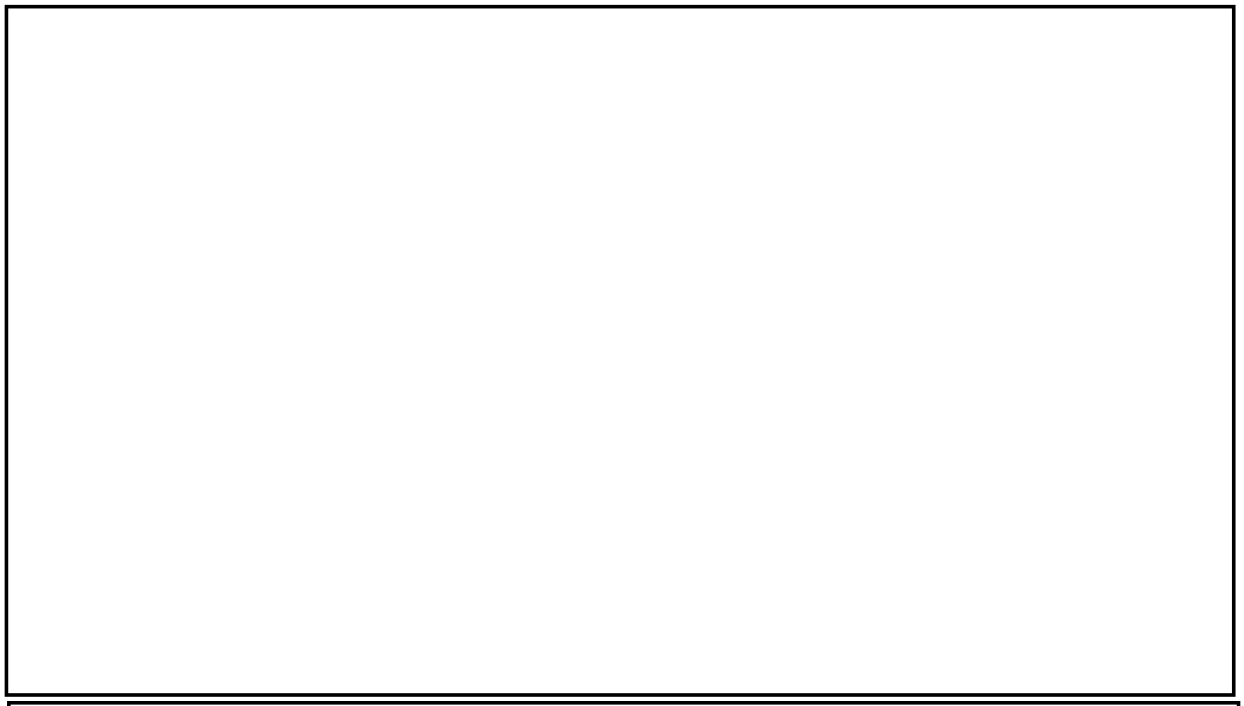
b5

11.

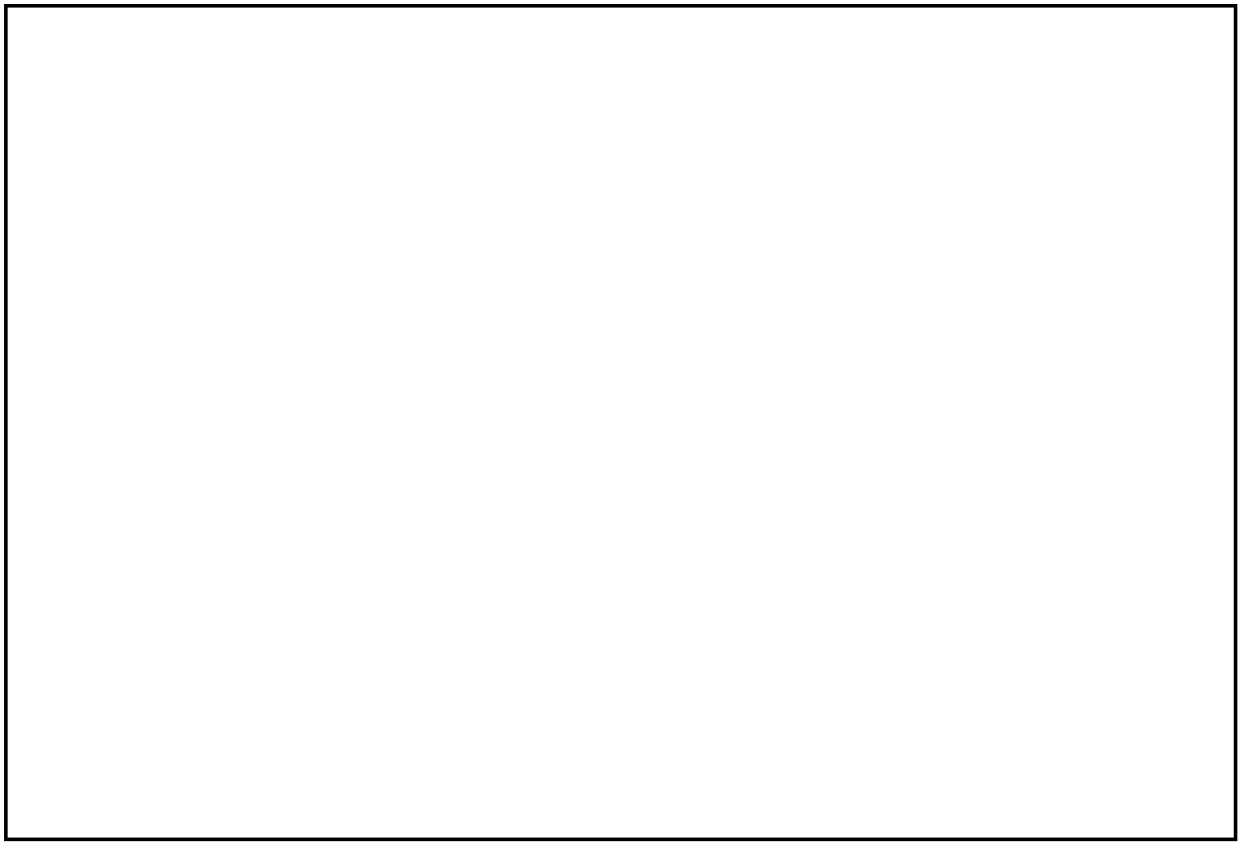
- 

b5

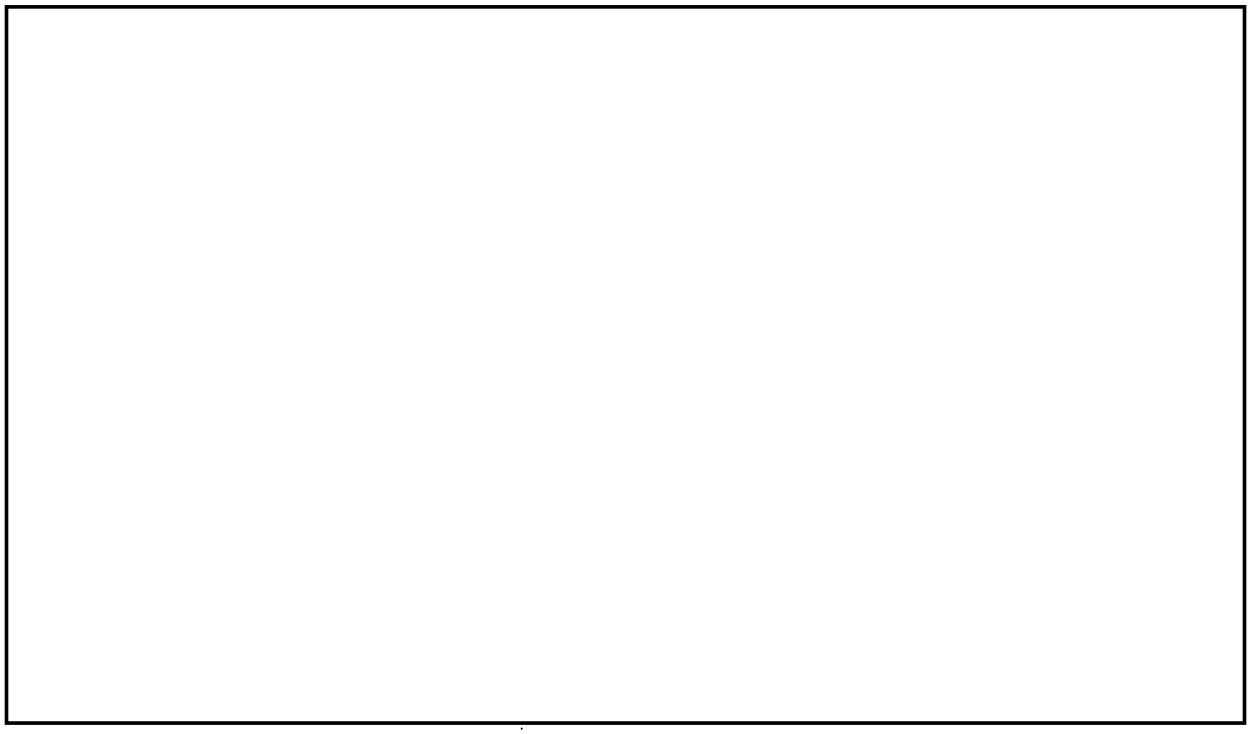
USA PATRIOT Act and Libraries



b5



b5



b5

(Draft responses to Sen. Judiciary Q's, 08/20/2002)

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/29/2002

To: Counterterrorism **Attn:** Section and Unit Chiefs
Counterintelligence Section and Unit Chiefs

From: Office of the General Counsel
National Security Law Unit (NSLU)/Room [redacted]
Contact: [redacted]

Approved By: Bowman M E
[redacted] b2

Drafted By: [redacted] b6 b7C

Case ID #: 66F-HQ-A1247863 (Pending)

Title: PROCEDURAL GUIDANCE RELATED TO
NEW FISA PEN REGISTER AUTHORITY

Synopsis: Summarizes FISA pen register/trap and trace authorities and reiterates procedures for requesting such authority.

Reference: 66F-HQ-A1247863 Serial 70

Administrative: This is a privileged FBI attorney communication; do not circulate outside the FBI without the permission of OGC.

Details: Changes to FISA pen register/trap and trace authorities under the "USA Patriot Act" were summarized in the above referenced electronic communication. In response to requests for clarification of procedures relating to requests for FISA pen register/trap and trace authorities, the National Security Law Unit (NSLU) is providing the following guidance.

I. Legal Basis for Initiation of FISA Pen Register/Trap and Trace

The "USA Patriot Act" revised the legal standard for initiating a FISA pen register/trap and trace.[1] These Orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such

[1] 50 U.S.C. § 1842

investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution."[2]

Use of this technique is authorized in full investigations properly opened under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). The FCIG require that full foreign counterintelligence investigations be personally authorized by the relevant Special Agent in Charge, or Assistant Special Agent in Charge with exclusive responsibility for a specific foreign counterintelligence program following written notification to FBIHQ.

II. Process for Obtaining Pen Register/Trap and Trace Authority

No procedural changes were required as the result of revisions made by the "USA Patriot Act." Requests for pen register/trap and trace authority should be submitted with an

[redacted] b2 b7E

[redacted] b2 b7E

[redacted] and a brief statement explaining the nature of the investigation and the relevance to that investigation of the information sought through the pen register/trap and trace.

NSLU and OIPR plan to develop additional guidance to further streamline this process. Questions relating to these matters may be directed to Assistant General Counsel [redacted] b2 b6 b7C

[2] 50 U.S.C. § 1842(a)(1).

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to relevant personnel involved in FCI/IT investigations.

CC:

♦♦ 1 - Mr. Parkinson
1 - Mr. Bowman
1 - NSLU Attorneys

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

July 16, 2002

[redacted] b6 b7C

Dear [redacted]

Senator Barbara Mikulski requested the FBI to address your concerns regarding certain provisions of the "Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (Patriot Act). I will address two sections of the law that are relevant to your inquiry.

First, section 215 of the Patriot Act amended the business records provision found in Title V of the Foreign Intelligence Surveillance Act. With passage of the Act, Congress established "relevance" to an investigation pertaining to international terrorism or clandestine intelligence activities as the legal standard for exercising this authority.[1] Thus, law enforcement authorities may seek a court order for the production of business records (including papers, documents, and other books and records from a business or other entity) provided that the records relate to an investigation properly authorized under the Attorney General Guidelines for FBI foreign counterintelligence investigations.[2]

Furthermore, the Patriot Act explicitly states in section 215 that no investigation of a United States person can be conducted solely upon the basis of activities protected by the First Amendment to the Constitution. The FBI does not base investigations on how persons exercise their First Amendment rights.

---

[1] The prior standard established by Congress was relevance and "specific and articulable" facts giving reason to believe that the person to whom the records related was an agent of a foreign power.

[2] This authority can be used to obtain records from libraries and bookstores although it is not designed specifically for application to any particular categories of institutions or businesses.

[redacted] b6 b7C

Second, you referenced provisions in the law that apply to Internet Service Providers (ISPs). Under section 505 of the Patriot Act, Congress established the same legal standard for obtaining National Security Letters (NSLs) as it did for the business records authority. NSLs are administrative subpoenas which can be issued in foreign counterintelligence investigations properly authorized under guidelines issued by the Attorney General to obtain telephone and electronic communication records from telephone companies and ISPs, as well as records from financial institutions, and information from credit bureaus. Section 505 also states that no investigation of a United States person can be conducted solely upon the basis of activities protected by the First Amendment.

The FBI has significant experience in its foreign counterintelligence investigations with persons using public libraries for clandestine and anonymous communications via library Internet access. It is, therefore, critical that we have the ability to obtain records of those communications.

The laws which established the business record and the NSL authority contain provisions that prohibit officers, employees or agents of companies receiving such orders from disclosing to the individual under investigation or to persons outside the company the fact that the FBI has sought or obtained access to information or records. Such provisions are intended to protect the integrity of the lawfully authorized investigation.

The changes made by the Patriot Act were thoroughly discussed and considered by Congress before they were enacted and are designed to enhance our ability to safeguard national security. They represent, in our view, a principled approach to balancing individual liberties with public safety.

I hope this information is beneficial to your understanding of these important and timely issues.

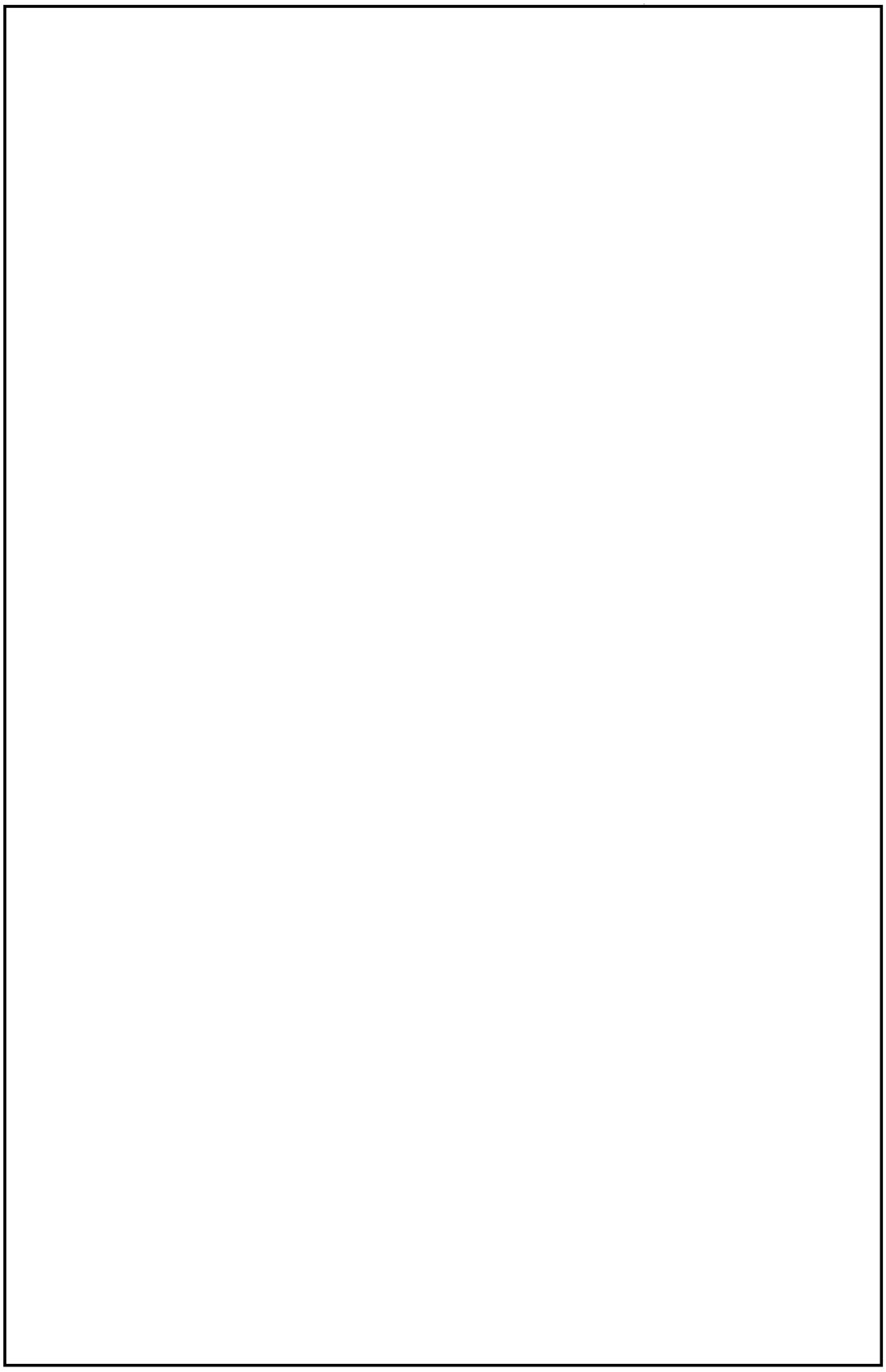
Sincerely yours,

M. E. Bowman
Deputy General Counsel
National Security Law Branch

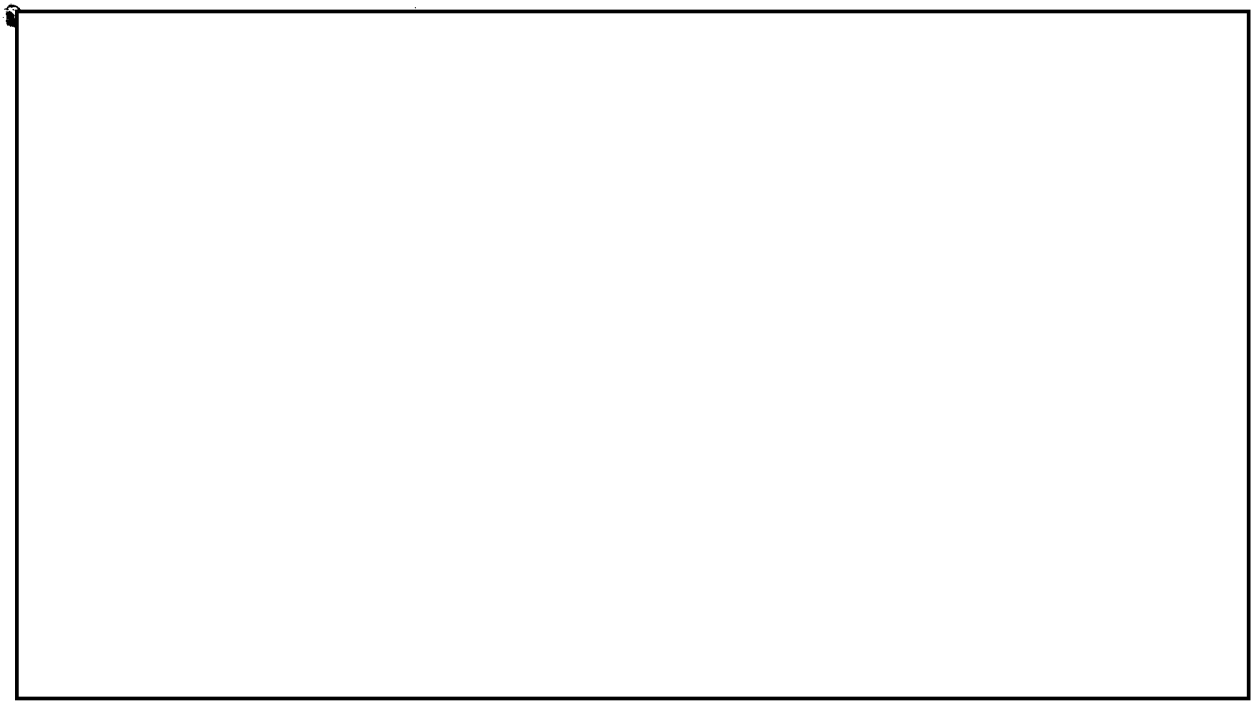
1 - [redacted] Staff Aide b6 b7C
U.S. Senator Barbara A. Mikulski
Hart Senate Office Building, Suite 709
Washington, D.C. 20510-2003

b5

Library/Bookstore Records

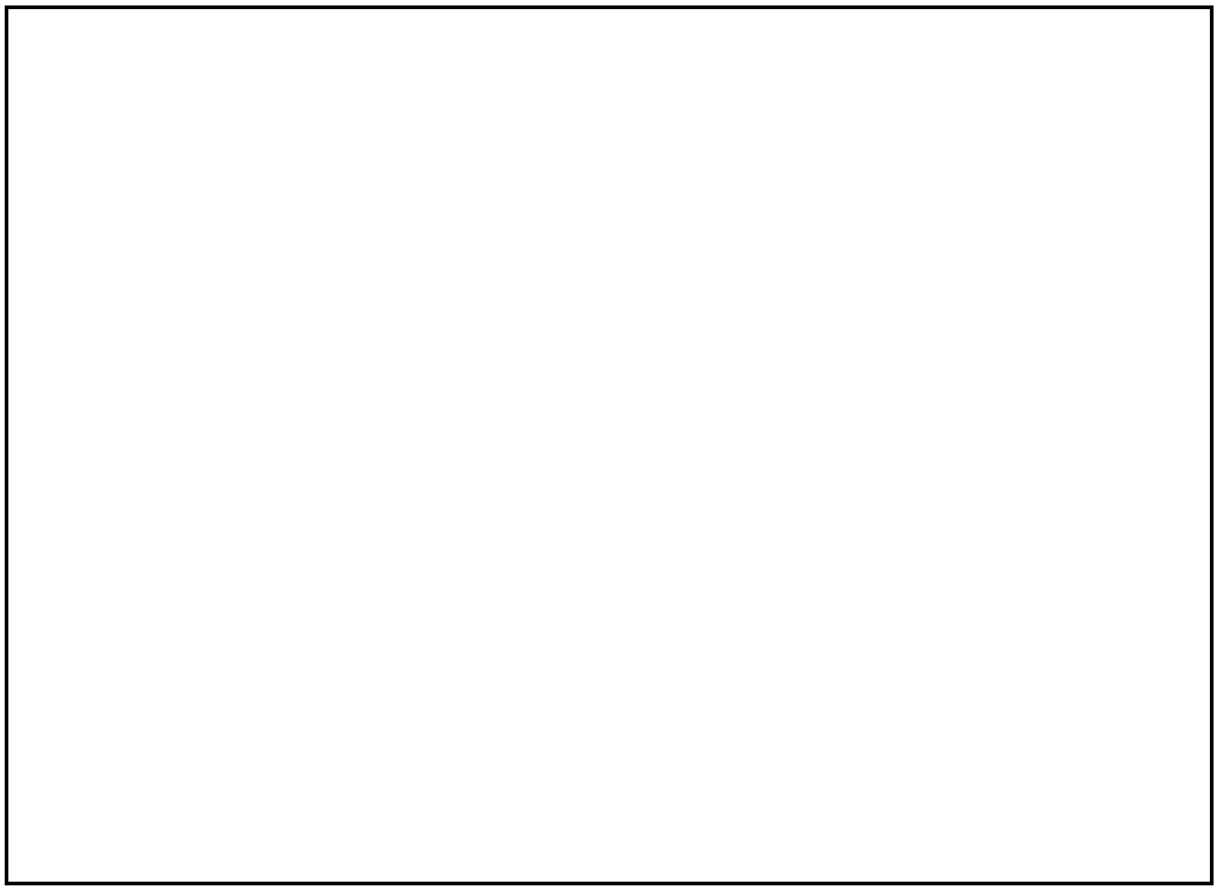


b5



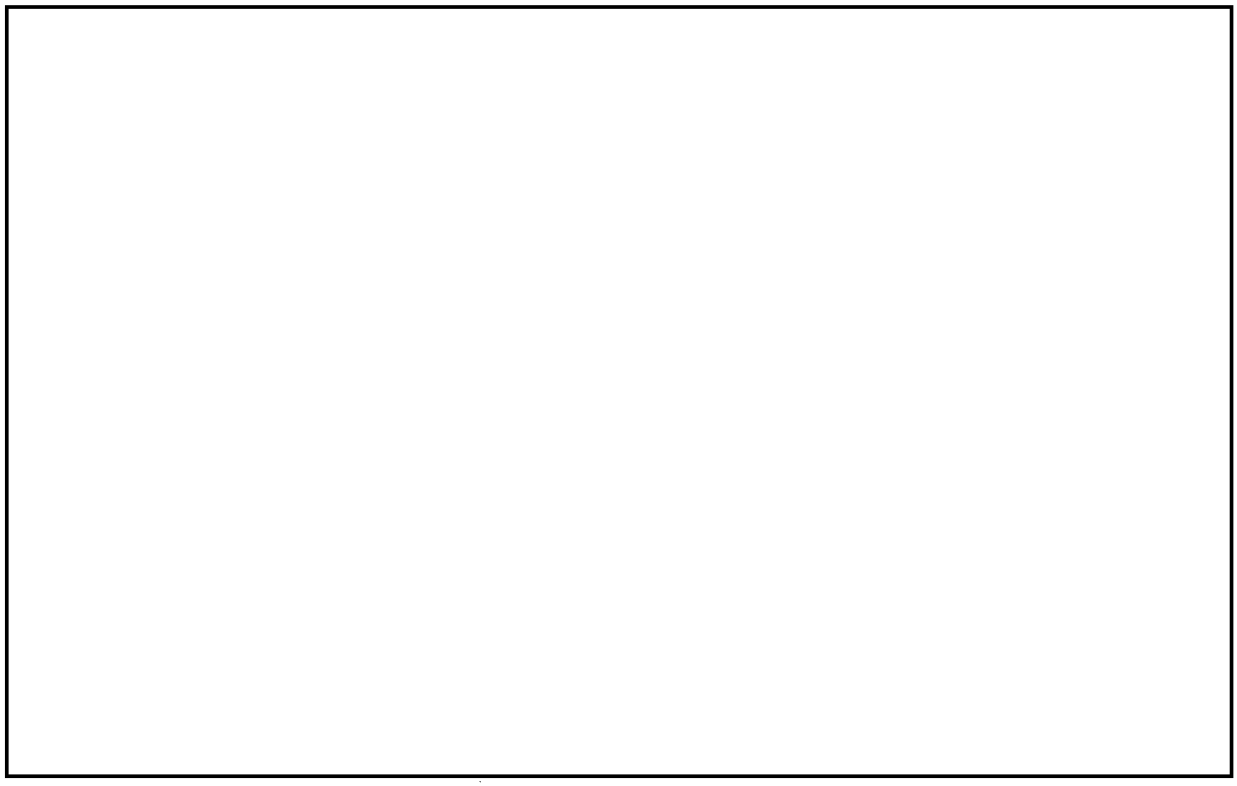
b5

(Draft QFRs, 01/30/2003)

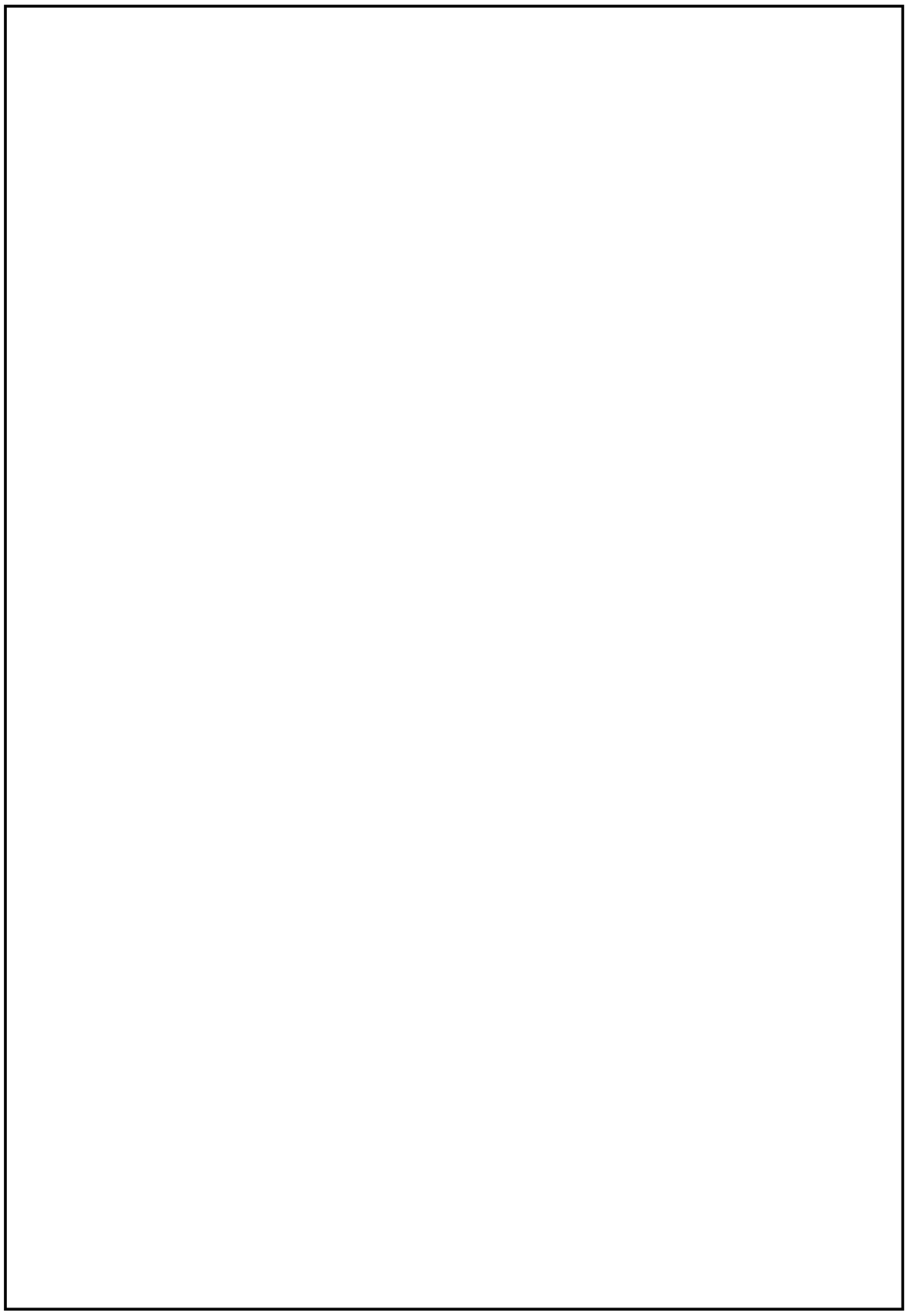


b5

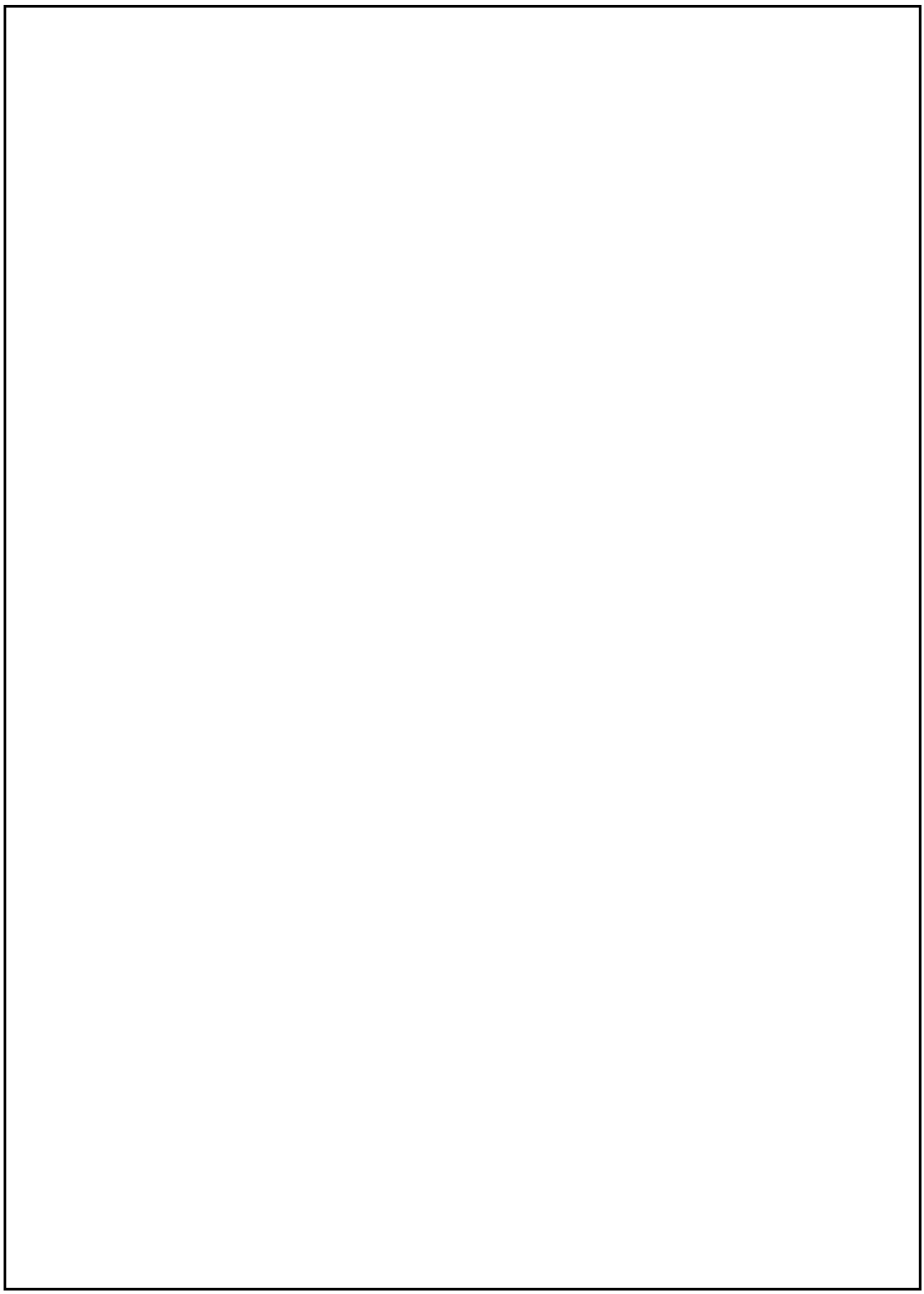
Questions from Senator Maria Cantwell



b5



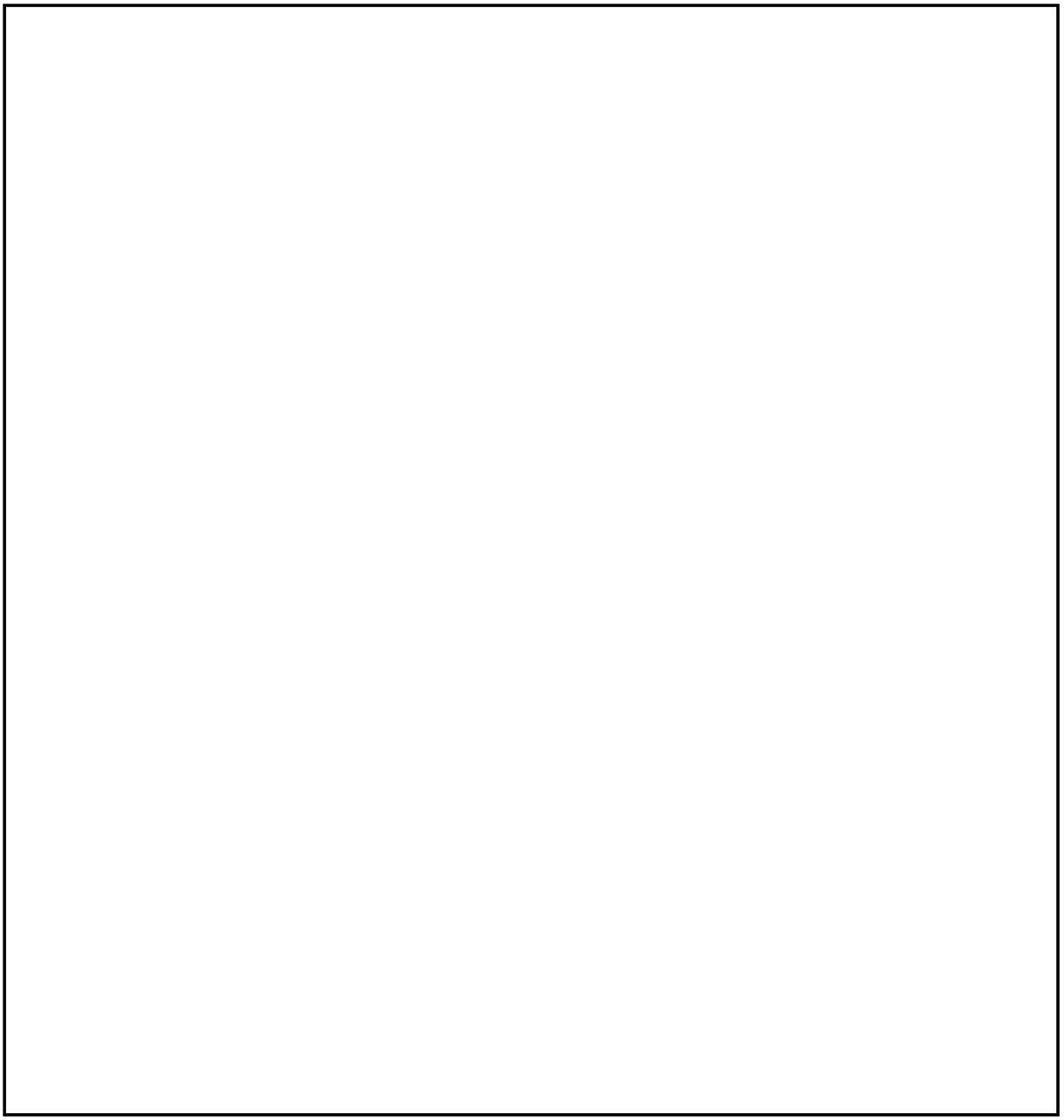
b5



b5

b5

Questions from Senator Russell Feingold



b5

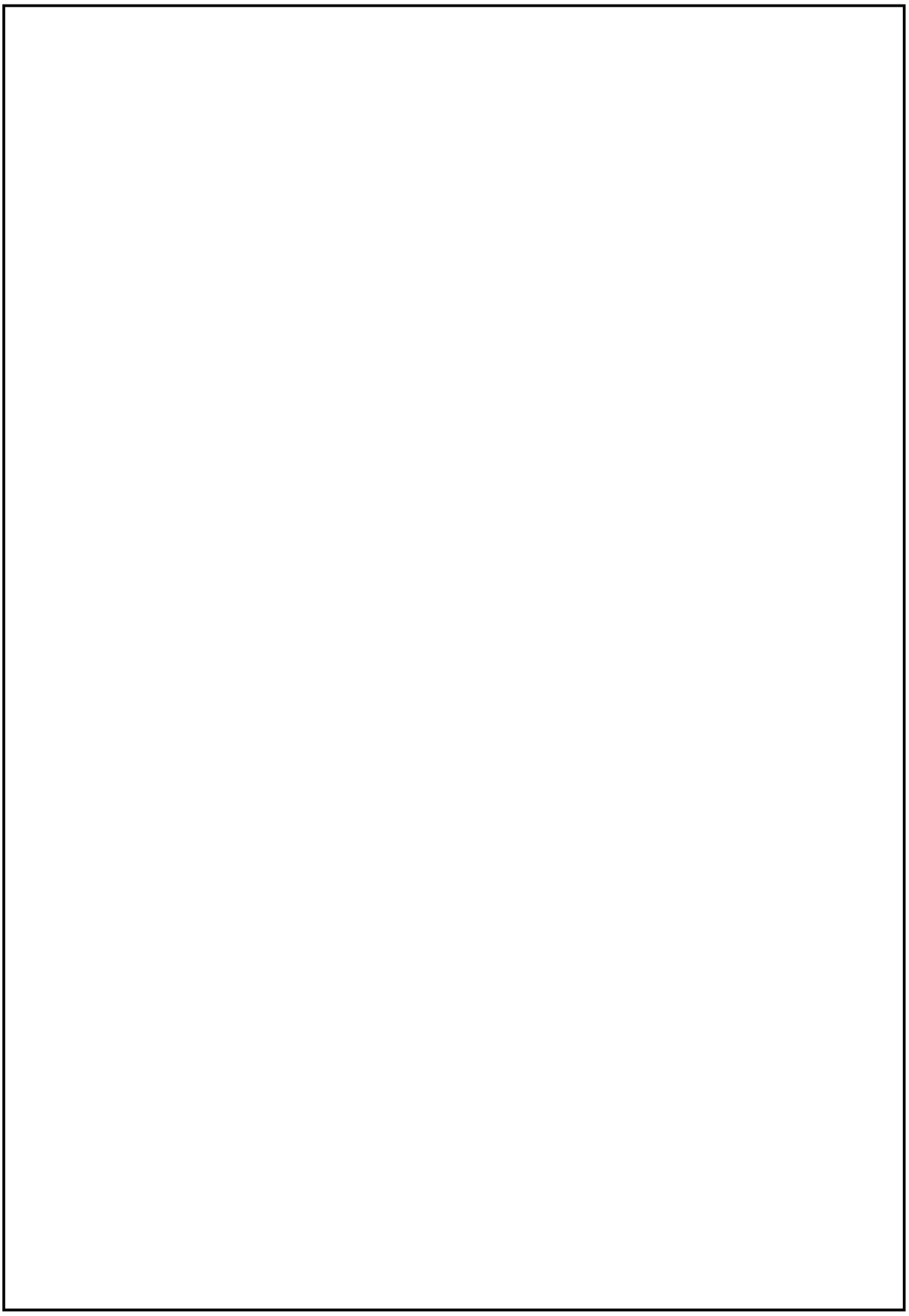
[redacted]

b5

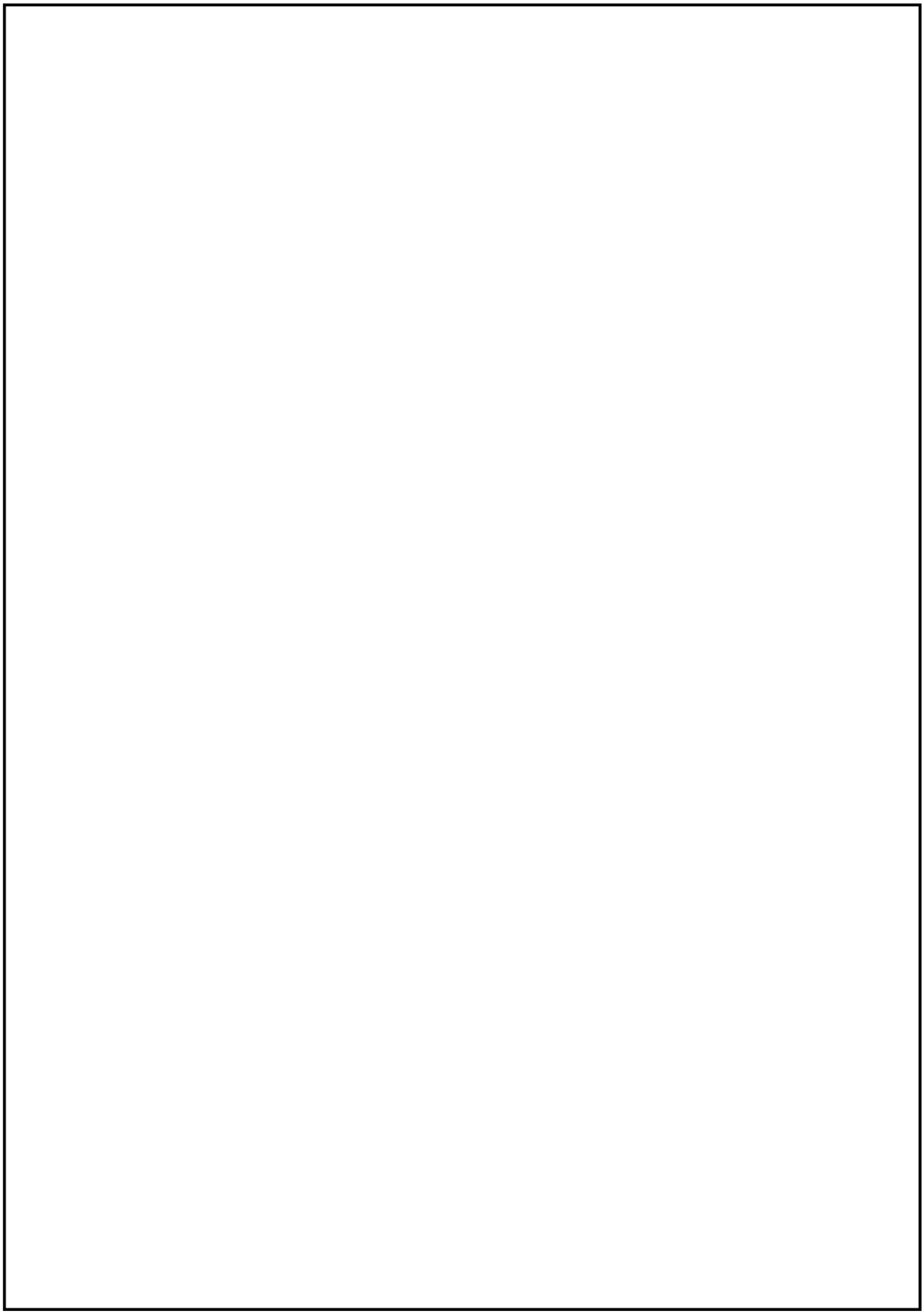
Questions from Senator Maria Cantwell

[redacted]

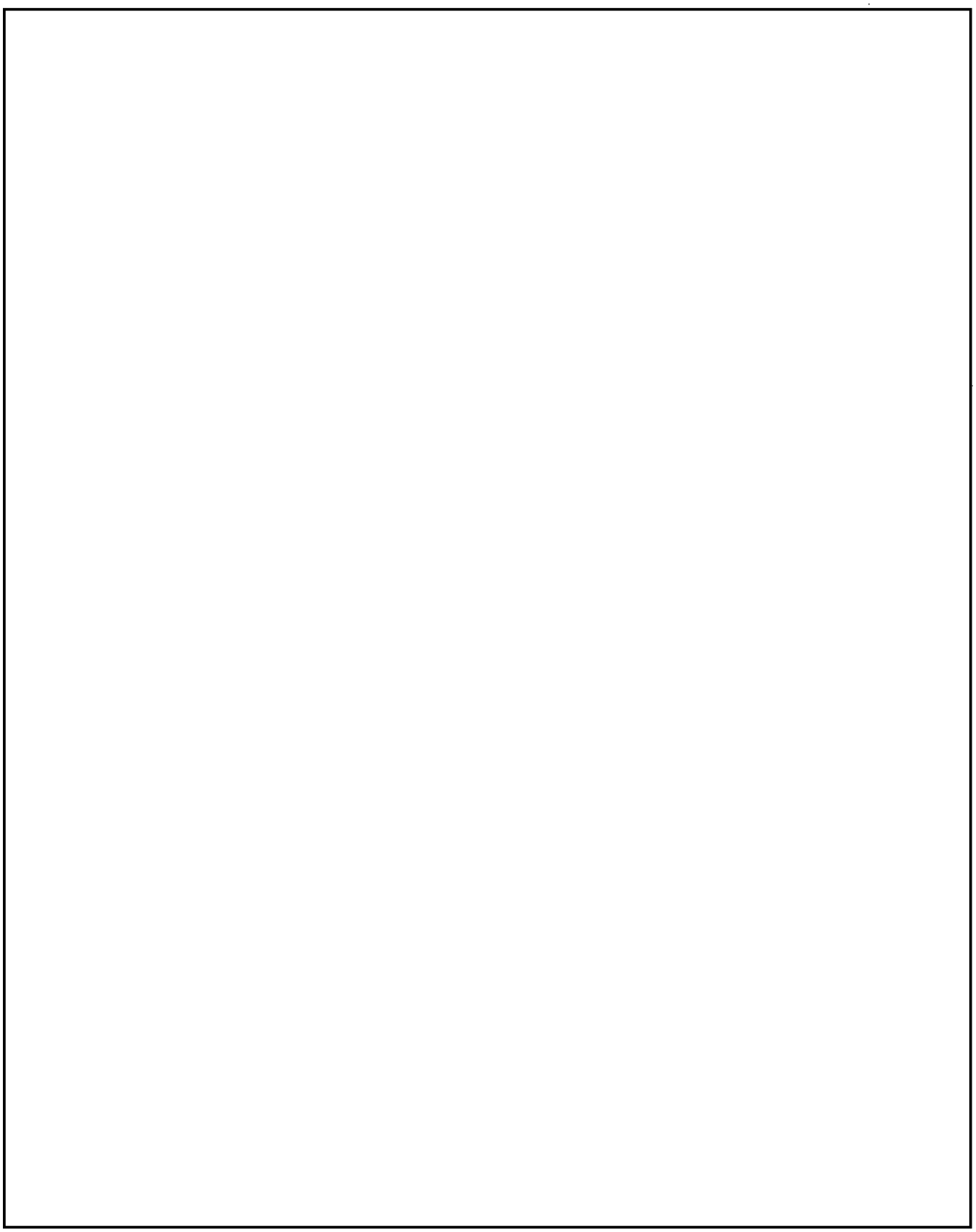
b5



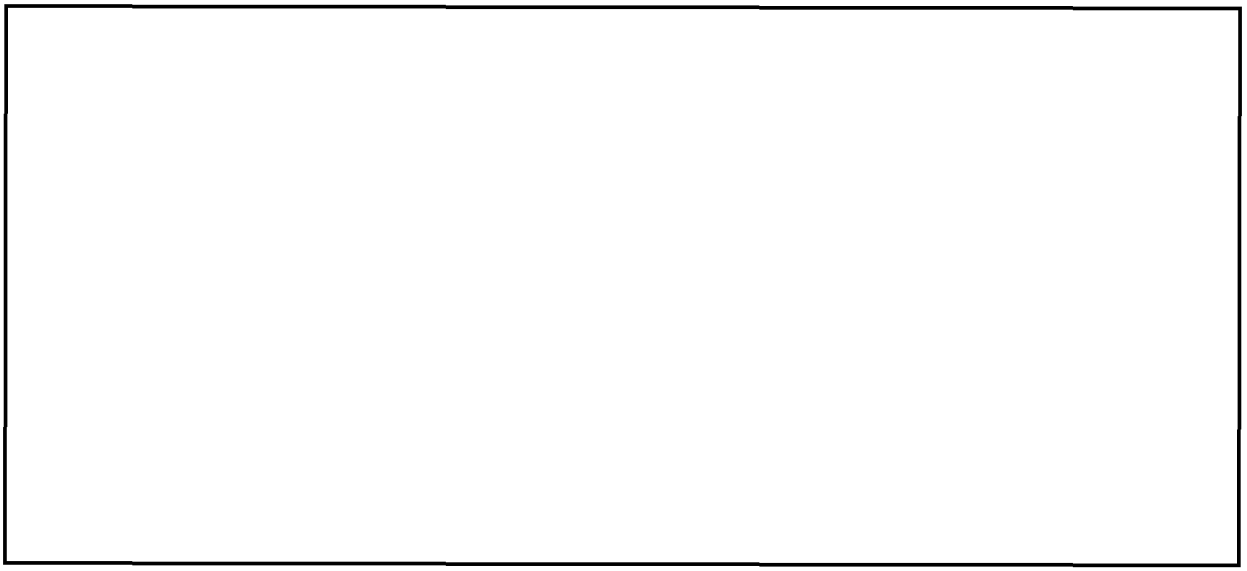
b5



b5



b5

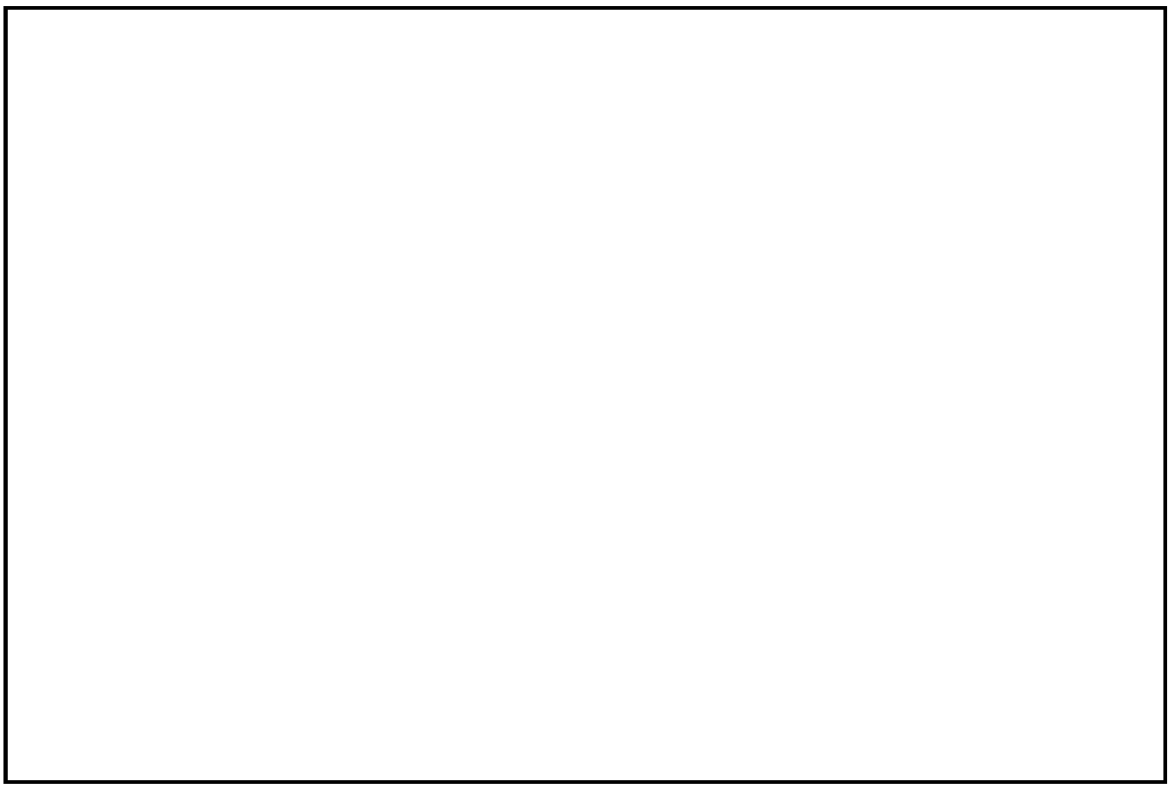


b5

(Draft responses to QFRs, 06/06/2002)

Questions from Senator Maria Cantwell

b5



b5

(Draft response to Sen. Cantwell, 01/24/2003)

[redacted] (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Thursday, March 10, 2005 6:01 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: Just getting back to you

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b2 b7E

I wanted to get back with you regarding my meeting with [redacted] this morning. We discussed [redacted] and their lack of movement. She admitted she has a stack of them on her desk because she removed them from [redacted] review. She hopes to have all of them reviewed by Monday. I am hopeful we will start to see movement again. We will see. I reminded her that Valerie has got to testify about our use of these probably in mid-April. I believe [redacted] will do her best, she is simply a voice crying out in the wilderness over there.

b6
b7C

On the threat list, where do we stand? Who is your contact in the substantive units? Keep me in the loop.

Julie F. Thomas
DGC, National Security Law Branch
Office of the General Counsel
Room 7975
202-324-8528
202-324-1023 (fax)
Julie.Thomas@ic.fbi.gov

UNCLASSIFIED

[redacted] (OGC) (FBI)

b6
b7C

From: GULYASSY, ANNE M. (OGC) (FBI)
Sent: Wednesday, October 20, 2004 9:16 AM
To: THOMAS, JULIE F. (OGC) (FBI); [redacted]
Cc: [redacted] (OGC) (FBI)
Subject: FW: ACLU's Position with regard to Section 215 of the PATRIOT Act:

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]ound this article in connection with ACLU's FOIA suits, but I thought you would find it interesting in terms of its discussion of Section 215 and NSLs generally. Anne

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Tuesday, October 19, 2004 6:32 PM
To: [redacted] HARDY, DAVID (RMD) (FBI); [redacted] GULYASSY, ANNE M. (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)
Subject: ACLU's Position with regard to Section 215 of the PATRIOT Act:

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I thought you would all find interesting the attached article in pdf I came across last night as I was surfing through the ACLU's website.

[redacted]

[redacted]
Assistant General Counsel
Office of the General Counsel
[redacted]

b2
b6
b7C

THIS IS A PRIVILEGED ATTORNEY-CLIENT/WORK PRODUCT COMMUNICATION AND IS NOT TO BE DISTRIBUTED OUTSIDE OF OGC WITHOUT PRIOR APPROVAL

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI)

From: Caproni, Valerie E. (OGC) (FBI) b6
Sent: Wednesday, March 30, 2005 11:51 AM b7C
To: [redacted] (OCA) (FBI)
Cc: KALISCH, ELENI P. (OCA) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Background Info for upcoming Patriot Act Hearings

UNCLASSIFIED
NON-RECORD

OIPR is compiling the numbers. Because DOJ is asking for the numbers through 3/31 the numbers will not be final until Friday. I will let OIPR know that we need the numbers ASAP.

In terms of the the background info, I think OIPR is doing that too.

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Wednesday, March 30, 2005 11:43 AM
To: Caproni, Valerie E. (OGC) (FBI) b6
Cc: KALISCH, ELENI P. (OCA) (FBI); [redacted] (OGC) (FBI) b7C
Subject: Background Info for upcoming Patriot Act Hearings

UNCLASSIFIED
NON-RECORD

Valerie - just to follow-up on our conversation yesterday re the DOJ decision to declassify certain data re use of specific provisions. Is OGC compiling #s (10/26/01 - 3/31/05) for the following provisions as enumerated in the draft Baker memo?

1. # of orders under §206 (roving fisa surveillance)
2. # of attorney hours at OIPR as a result of §207 extensions
3. # of PR/TT orders under §214 b2 b7E
4. # of orders under §215 (business records) - DOJ is planning to declassify total and #s within categories [redacted] info in conjunction with PR/TT.

The draft memo would declassify # of orders approved by the Court. I'm assuming that the total # of orders requested (either requested by FBI and not approved by DOJ or requested by DOJ and not approved by the Court) will remain classified?

Is OGC compiling background info re the cases approved in these categories? (i.e. if there were X §215 orders approved, can we identify the X cases and give the Director some background info?)

Sorry if this is redundant based on our conversation, but I wanted to confirm what info is being gathered. Thanks,

[redacted]
Office of Congressional Affairs b2
[redacted] b6
b7C

6/17/2005

UNCLASSIFIED

[redacted] OGC) (FBI)

From: [redacted] (OCA) (FBI)
Sent: Wednesday, March 30, 2005 11:43 AM
To: Caproni, Valerie E. (OGC) (FBI)
Cc: KALISCH, ELENI P. (OCA) (FBI); [redacted] (OGC) (FBI)
Subject: Background Info for upcoming Patriot Act Hearings

b6
b7C

UNCLASSIFIED
NON-RECORD

Valerie - just to follow-up on our conversation yesterday re the DOJ decision to declassify certain data re use of specific provisions. Is OGC compiling #s (10/26/01 - 3/31/05) for the following provisions as enumerated in the draft Baker memo?

1. # of orders under §206 (roving fisa surveillance)
2. # of attorney hours at OIPR as a result of §207 extensions
3. # of PR/TT orders under §214
4. # of orders under §215 (business records) - DOJ is planning to declassify total and #s within categories - i.e. [redacted] info in conjunction with PR/TT.

b2 b7E

The draft memo would declassify # of orders approved by the Court. I'm assuming that the total # of orders requested (either requested by FBI and not approved by DOJ or requested by DOJ and not approved by the Court) will remain classified?

Is OGC compiling background info re the cases approved in these categories? (i.e. if there were X §215 orders approved, can we identify the X cases and give the Director some background info?)

Sorry if this is redundant based on our conversation, but I wanted to confirm what info is being gathered. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Thursday, March 17, 2005 12:55 PM b7C
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted]

Subject: Patriot act provision re: public libraries

UNCLASSIFIED
NON-RECORD

CTD is assisting Office of Congressional Affairs prepare the Director for testimony re: patriot act and its sunset provision (December, 2005?). You are probably going to be getting questions about success stories related to the changes made by the Act. One question I have gotten is about the provision permitting the FBI to review records at a public library. CTD is having difficulty determining if this was ever utilized. Does anyone know?

I haven't even been able to determine what the procedure would have been for anyone seeking to use this provision, does anyone know what the process would be?

[redacted]
NSLB - CTLU 1
[redacted] b2 b6 b7C

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Thursday, March 17, 2005 7:30 AM b7C
To: [redacted]
(OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

Here is the e-mail which [redacted] is responding to b6 b7C

Do we have PAtriot Act successes.

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Wednesday, March 16, 2005 2:49 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] Caproni, Valerie E. (OGC) (FBI)
Subject: RE: Two things

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] it sounds like you've got the ticket to start drafting testimony for the Director to use for the Senate Judiciary Committee Patriot Act hearing scheduled for 4/5/2005. See attached e-mail to GC Caproni with relevant dates - OCA needs to see a draft of the testimony by Tues, 3/22.

[redacted] b5

Give me a call to discuss. Thanks,

[redacted]
National Security Law Policy and Training Unit
FBI HQ Room [redacted]
[redacted] b2 b6 b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 17, 2005 7:26 AM
To: [redacted] (OGC) (FBI);

(OGC) (FBI)
Subject: RE: Draft Testimony re Patriot Act

UNCLASSIFIED
NON-RECORD

b2
b6
b7C

Could you get operaitonal examples for n for this project which we are doing for Congressional Affairs.

National Security Law Policy and Training Unit
FBI HQ Roon

-----Original Message-----
From: (OGC) (FBI)
Sent: Wednesday, March 16, 2005 3:39 PM
To: OCA) (FBI)
Subject: RE: Draft Testimony re Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

If you need operational examples please get them through

b2
b6
b7C

National Security Law Policy and Training Unit
FBI HQ Roon

-----Original Message-----
From: OCA) (FBI)
Sent: Wednesday, March 16, 2005 3:36 PM
To (OGC) (FBI)
Cc: OGC) (FBI); Caproni, Valerie E. (OGC) (FBI); KALISCH, ELENI P. (OCA) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: Draft Testimony re Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

attached is some info that might assist in drafting testimony.
1. Testimony of RSM 2004 - the Patriot Act was just a piece of more general testimony, but this gives you a flavor of the tone of his testimony.
2. Sunsets Report Final Draft - I expect that the AG's testimony for the 4/5 hearing will draw heavily from this document that was prepared by DOJ OLP. For that reason and because it primarily is a legal analysis (v. practical), I don't think that we should rely heavily on it, but it

might be helpful.
3. DOJ Patriot Act Report - I think Section II of this report might be a good place to start. It contains some examples, but they might be a bit tired / overused. See next doc for additional examples.
4. Sunset - field input - This doc was based on an OGC survey and contains case examples for many of the provisions. The problem is that DOJ will not clear testimony that has pending case examples... still, there might be something that we can use.

After you've had a chance to review, please give me a call and we can chat.

[redacted]
Office of Congressional Affairs b6
[redacted] b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 12
Page 2 ~ Duplicate
Page 3 ~ Duplicate
Page 4 ~ Duplicate
Page 5 ~ Duplicate
Page 6 ~ Duplicate
Page 7 ~ Duplicate
Page 8 ~ Duplicate
Page 9 ~ Duplicate
Page 10 ~ Duplicate
Page 11 ~ Duplicate
Page 133 ~ Duplicate
Page 134 ~ Duplicate

~~Patriot~~ Act

I. The USA PATRIOT Act has proved invaluable in helping the FBI's mission of fighting terrorism in the United States and abroad.

A. It has torn down the wall between the FBI criminal and intelligence investigators by allowing the timely sharing of information to fight terrorism collectively.

B. It has increased the sharing of information between the FBI and other intelligence agencies.

C. It has permitted the sharing of grand jury and Title III information with intelligence officials.

D. It has permitted Special Agents in Charge of the field offices to issue National Security Letters (NSLs) for telephone/toll records, electronic communications records, subscriber information, financial records, and certain credit information under a standard of "relevance" to an authorized national security investigation.

E. It has lowered the standard for a FISA pen register/trap& traces to "relevance" to an authorized investigation; coupled with revisions to the Attorney General's Guidelines for National Security Investigations, this allows for use of pen registers/trap & trace in Preliminary Investigations.

F. It has permitted the use of roving FISA wiretaps.

G. It has given federal judges authority to issue search warrants that are valid outside the issuing judge's district in terrorism investigations.

H. It has given FBI investigators authority to obtain full credit reports via a NSL-type letter for terrorism investigations.

I. It has increased the number of FISA judges from seven to 11 to help accommodate the increased number of counterterrorism FISAs; and

J. It has amended the material support to terrorism statutes to expand the FBI's ability to arrest financial supporters of terrorism.

II. Retain intelligence provisions in the PATRIOT Act that are subject to sunset

A. Sec. 201. Authority to intercept wire, oral, and electronic communications

relating to terrorism

B. Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.

C. Sec. 203. Authority to share criminal investigative information.

D. Sec. 203(b) (Title III) and (d) (Grand Jury)

E. Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.

F. Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

G. Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.

H. Sec. 212. Emergency disclosure of electronic communications to protect life and limb.

I. Sec. 214. Pen register and trap and trace authority under FISA.

J. Sec. 215. Access to records and other items under the FISA.

K. Sec. 217. Interception of computer trespasser communications.

L. Sec. 218. Foreign intelligence information. Section 218 is the section that sets the "significant purpose" standard in FISA. Should section 218 expire, the November 18, 2002 FISA Court of Review Opinion would become the legal standard for the initiation and continuation of FISA searches and surveillances. The Court of Review upheld the "significant purpose" standard, but absent the language of the USA PATRIOT Act, the purpose of FISA searches and surveillance will become intelligence collection, no matter what other purpose may exist. It can be argued that this change would be a narrower, more restrictive standard than the USA Patriot Act created."

III. What other legislative changes are needed?

A. National Security Letters (NSLs)

1. Create an enforcement mechanism.

a. The statutes providing for NSLs lack enforcement provisions. As a result, some record holders do not comply. Changes to the NSL statutes are already being considered by DOJ due to

Patriot Act

I. The USA Patriot Act has proved invaluable in helping the FBI's mission to fight terrorism in the United States and abroad.

A. It has torn down the wall between the FBI criminal and intelligence investigators by allowing the timely sharing of information to fight terrorism collectively.

B. It has increased the sharing of information between the FBI and other intelligence agencies.

C. It has permitted the sharing of grand jury and Title III information to intelligence officials.

D. It has permitted the field office Special Agents in Charge to issue National Security Letters (NSLs) under a relevance to an FBI investigation standard for telephone/toll records, electronic communications records, subscriber information, financial records, and certain credit information.

E. It has lowered the standard for a FISA pen register/trap& traces to "relevance" to an authorized investigation; coupled with revisions to the Attorney General's Guidelines for National Security Investigations, this allows for use of pen registers/trap & trace in Preliminary Investigations.

F. It has permitted the use of roving FISA wiretaps.

G. It has given federal judges authority to issue search warrants that are valid outside the issuing judge's district in terrorism investigations.

H. It has given FBI investigators authority to obtain full credit reports via a NSL-type letter for terrorism investigations.

I. It has increased the number of FISA judges from seven to 11 to help accommodate the increased number of counterterrorism FISAs; and

J. It has amended the material support to terrorism statutes to expand the FBI's ability to arrest financial supporters of terrorism.

II. Retain intelligence provisions in Patriot Act that are subject to sunset

A. Sec. 201. Authority to intercept wire, oral, and electronic communications relating to terrorism

B. Sec. 202. Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.

C. Sec. 203. Authority to share criminal investigative information.

D. Sec. 203(b) (Title III) and (d) (Grand Jury)

E. Sec. 204. Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.

F. Sec. 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

G. Sec. 207. Duration of FISA surveillance of non-United States persons who are agents of a foreign power.

H. Sec. 212. Emergency disclosure of electronic communications to protect life and limb.

I. Sec. 214. Pen register and trap and trace authority under FISA.

J. Sec. 215. Access to records and other items under the FISA.

K. Sec. 217. Interception of computer trespasser communications.

L. Sec. 218. Foreign intelligence information. Section 218 is the section that sets the "significant purpose" standard in FISA. It should be noted that should this expire, the November 18, 2002, FISA Court of Review Opinion would set the FISA standard. The Court of Review upheld the "significant purpose" standard, but if the Patriot Act goes away, you would be left with the Court of Appeals standard that a purpose be intelligence, no matter what other purpose you have. It could be argued that this standard is lower than the Patriot Act.

III. What other legislative changes are needed?

A. Amend FISA Statute 1806(b) and 1825(c) required caveats.

1. Revise the FISA caveat requirement so that FISA-derived information may be shared for terrorism screening and "lead purposes" without the need to include a statement that such information may only be used in a criminal proceeding with the advance authorization of the AG. In the current era of information sharing, inclusion of this language is a red flag signaling the use of FISA techniques. Moreover, if the information is disseminated only

[redacted] (OGC) (FBI)

From: [redacted] (INSD) (FBI) b6 b7C
Sent: Wednesday, July 21, 2004 8:21 AM
To: FOGLE, TONI M. (INSD) (FBI); [redacted] (INSD) (FBI); [redacted] (OPR) (FBI); [redacted] (OPR) (FBI); [redacted] (OPR) (FBI)
Cc: [redacted] OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (INSD) (FBI)
Subject: RE: Questions for the Record from Director's 5/20/04 Senate Hearing

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-17-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

We no longer have to reply to the last question re non-content communications. b6 b7C

[redacted]

-----Original Message-----
From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, July 20, 2004 8:24 PM
To: [redacted] (INSD) (FBI); [redacted] (OPR) (FBI); [redacted] OPR) (FBI); [redacted] (OPR) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (INSD) (FBI); [redacted] INSD) (FBI)
Subject: Questions for the Record from Director's 5/20/04 Senate Hearing

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] (system search) -- b6 b7C

I have been asked to respond to an urgent request from OCA -- and I need to know the following:

Has the FBI (they also ask about DOJ and DCI -- but I wouldn't even know where to go to get those responses)

--received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 215 of the USA-Patriot

Act?

--received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act?

If so, describe the disposition of any such complaint.

We were also asked to respond to the following question -- but I'm not sure we are the appropriate responding entity:

"Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee."

Please let me know positive and negative fast -- (we were missed in the original dissemination).

[redacted] - I copied you guys just in case you knew of something out there we weren't aware of.}

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

b6
b7C

[redacted] (OGC) (FBI)

From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, July 20, 2004 8:24 PM
To: [redacted] (INSD) (FBI); [redacted] (OPR) (FBI); [redacted] (OPR) (FBI); [redacted] (OPR) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (INSD) (FBI); [redacted] (INSD) (FBI)
Subject: Questions for the Record from Director's 5/20/04 Senate Hearing

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-17-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] (system search) --

I have been asked to respond to an urgent request from OCA -- and I need to know the following:

Has the FBI (they also ask about DOJ and DCI -- but I wouldn't even know where to go to get those responses)

--received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act?

--received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act?

If so, describe the disposition of any such complaint.

We were also asked to respond to the following question -- but I'm not sure we are the appropriate responding entity:

"Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee."

Please let me know positive and negative fast -- (we were missed in the original dissemination).

b6
b7C

[redacted] -- I copied you guys just in case you knew of something out there we weren't aware of.}

SENSITIVE BUT UNCLASSIFIED

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 07/19/2004 **Date:** 06/09/2004

To: Counterterrorism	**Attn:**	AD Bald DAD Harrington
		[redacted]
General Counsel	**Attn:**	General Counsel Caproni DGC Kelley
International Operations	**Attn:**	SAC Fuentes
Laboratory	**Attn:**	AD Adams DAD Hildebrand
CJIS	**Attn:**	AD Kirkpatrick DAD Hooks
Director's Office	**Attn:**	CIO Azmi Acting OPR AD Dzwilewski
Office of Intelligence	**Attn:**	EAD Baginski
		[redacted]
Security	**Attn:**	AD Phalen DAD Berkin
Criminal Investigative	**Attn:**	Acting AD Lewis DAD Swecker
Counterintelligence	**Attn:**	AD Szady DAD Andress
Records Management	**Attn:**	AD Hooton DAD Hendershot

b6
b7C

From: Office of Congressional Affairs
Room 7240
Contact: [redacted]

b2
b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-18-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

Approved By: Powers Richard C

Drafted By: [redacted]

Case ID #: 62F-HQ-1077726 Serial 321

Title: QUESTIONS FOR THE RECORD FOLLOWING
THE DIRECTOR'S MAY 20, 2004 HEARING
BEFORE THE SENATE JUDICIARY COMMITTEE

Synopsis: To request responses to Questions for the Record submitted by the Senate Committee on the Judiciary following the Director's 5/20/04 oversight hearing.

Details: The Senate Committee on the Judiciary has posed many Questions for the Record based on the Director's 5/20/04 oversight hearing. Those questions are provided, verbatim, below, along with an indication of the Division we believe most likely to possess responsive information. Many of these

questions have subparts. If no assignment is made with respect to the subparts of a given question, they are to be answered with the main question. If you believe a specific question would be more appropriately directed to another entity, please contact [redacted] ext. [redacted] for reassignment of the question. b2 b6 b7C

Please make every effort to avoid classified responses. If a classified response is necessary, please clearly mark that information so that it can be transmitted to the Committee separately. In addition, if pending case information will be involved, please indicate any such information that would preclude us from answering. These responses will be coordinated with DOJ before transmission to the Committee.

The Committee's questions follow.

Questions Posed by Senator Hatch

On May 24, 2004, the FBI National Press Office issued a press release regarding the misidentification and release from custody of Brandon Mayfield. I am concerned that the FBI arrested an American citizen, incarcerated him, and subsequently released him from custody because of a misidentified fingerprint.

1. Laboratory Division (LD) (in coordination with the Counterterrorism Division (CTD)). In order to more fully understand this issue, please provide a chronology of events leading up to the misidentification of Mr. Mayfield. Include in this chronology an explanation of the events leading up to the initial identification of Brandon Mayfield as well as the circumstances that led to acknowledgement that Mayfield had been misidentified. Specifically, what efforts were made to secure the original or best fingerprint evidence? How many requests were made? Was there any attempt to utilize the actual prints held by the authorities in Spain? How many visits to Spain were made regarding the fingerprints in question? When was Mr. Mayfield officially identified? At what point did the FBI become aware of the doubts of the Spaniards as to Mr. Mayfield being the owner of the prints in question? When did the FBI discover the misidentification? What actions were taken immediately following the misidentification?

2. LD.

a. Please describe the standard protocols and methodologies that FBI fingerprint examiners use to determine whether a particular latent fingerprint is of value for

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeapor[dize] an investigation or unduly [delay] a trial" been used? Please describe the circumstances in each of these cases?

83. Sections 201 and 202 of the USA-Patriot Act added a number of offenses to the "predicate offense list" applicable to criminal wiretaps pursuant to Chapter 119 of Title 18. The following question pertains to the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. OGC. In how many cases has have the newly-added predicate offenses been used to support an application for a criminal wiretap under the authority of Chapter 119 of Title 18?

b. OGC. In how many such cases has the newly-added predicate offense been the only predicate offense asserted as the basis for the warrant, i.e., where a warrant could not have been lawfully issued but for the passage of the additional criminal predicates?

c. Inspection Division. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Sections 201 or 202 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

d. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute, including the addition of predicate crimes, which the Congress should consider?

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. OGC. How often has this authority been used, and with what success?

b. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Some have read this section as providing for surveillance in cases where neither the identify of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

d. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act? If so, please describe the nature and disposition of such a complaint.

e. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. OGC. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

b. OGC. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate?

c. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

d. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

87. Section 209 of the USA-Patriot Act clarified the law with regarding the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. OGC. How many such search warrants have been issued since passage of this act?

b. OGC. In such cases, have there been any instances in which a wiretap, as opposed to a search, warrant would not

have been supported by the facts asserted in support of the search warrant.

c. Inspection Division. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

d. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

88. Section 212 of the USA-Patriot Act permits communications service providers to provide customer records or the content of customer communications to the FBI in an emergency situation. This question pertains to application of this provision since its passage, and to all instances, not only to terrorism investigations.

a. OGC. In how many cases has this provision been used? Please provide a short description of each such case to the Committee.

b. OGC. In any such case have there been any cases in which, except for the time constraints imposed by the emergency situation, a conventional wiretap or search warrant, would not have been supported by the facts available to the Government at the time of the emergency request? If so, please describe such situations.

c. Inspection Division. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

d. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

(i) How many of such cases were terrorism-related?

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and

lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

91. Section 217 of the USA-Patriot Act authorizes, without court order, the interception of communications to and from a trespasser with a protected computer. This question pertains to the implementation of this provision since its passage.

a. OGC. How many times has the authority under this section been used, and with what success? Please provide descriptions of the circumstances where it has been used.

b. OGC. Section 217(2)(I) requires authorization by the owner of the computer before the section can be applied. Can this authorization be withdrawn or limited by the owner of the computer? If so, how and in what circumstances?

c. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

93. Section 220 of the USA-Patriot Act, "Nationwide Service of Search Warrants for Electronic Evidence" allows for the execution of a search warrant seeking electronic data anywhere in the country. This question pertains to the implementation of this provision since its passage.

a. OGC. In how many cases has this authority been used?

b. Inspection Division. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 220 of the

USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

94. OGC. Section 223 of the USA-Patriot Act creates a cause of action for willful violations of Title III's electronic surveillance procedures. Have any such lawsuits been brought? If so, please provide details of each such case.

95. OGC. Section 225 of the USA-Patriot Act provides immunity for those who aid in the execution of a FISA order. Has such immunity been invoked? If so, please describe any such case.

96. The following question pertains to surveillance conducted pursuant to the FISA.

a. CTD. What is the backlog on processing of intercepts? What is the average time between interception and first monitoring.

b. OIO. What percentage of intercepts that are not in English are translated within 24 hours? A week?

c. OIO. How many hours of FISA intercepts remain untranslated as of May 20, 2004?

d. CTD. Please describe the process of indexing and retrieving FISA material.

e. OIO. In the past 5 years, has there been a review or audit of the accuracy of FBI translations of intercepted or seized foreign language material?

Questions Posed by Senator Feingold

FBI Role in Iraq

97. OIO.

a. How many special agents, translators, and other FBI employees have been assigned to work in Iraq since March 2003 and how many are currently there ?

b. Where were these agents, translators, and other employees assigned before they were sent to Iraq?

asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

104. CTD. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518(11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

b. The SAFE Act would also require the FBI to identify either the target of the wiretap or the place to be wiretapped. For example, in the event that the FBI has a physical description of the target but does not know the identity of the target, the SAFE Act would allow the FBI to conduct a "John Doe" wiretap by identifying the facilities to be wiretapped. This is a sensible requirement to protect innocent Americans who are not the target of an investigation, while still allowing the FBI to conduct surveillance of suspected terrorists or spies. Why shouldn't Congress enact this prudent safeguard? Please explain.

Questions Posed by Senator Durbin

105. Finance Division. You testified that terrorism prevention is the top priority of the Bureau and that resources have been diverted within the Bureau in support of this important effort. However, the fight against terrorism should not come at the cost of diminished law enforcement in critical areas such as criminal civil rights violations. Please discuss what resources if any have been diverted away from the FBI's Civil Rights Program since September 11, 2001.

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, July 15, 2004 8:33 AM
To: [redacted] (OGC) (FBI)
Subject: Answer to SSCI Question 34

b6
b7C

UNCLASSIFIED
NON-RECORD

"Prior to the Patriot Act, the FISA statute was interpreted to require that there existed a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpetation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors. These procedures were often burdensome, but prior to the Patriot Act information was shared from intelligence investigations to criminal investigations. This sharing was often difficult and burdensome, but intelligence information was shared with criminal investigations."

UNCLASSIFIED

CERTIFICATE OF SERVICE OF ATTACHED ORDER

Date and Time of Service _____

Place of Service _____

Served upon _____

Served by _____

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Certificate of Service of Attached Order is true and correct.

Executed on _____ By: _____
Date Signature of Server

Inquiries Regarding Production May Be Directed to:

Name of Special Agent
Federal Bureau of Investigation
____ Field Office
Telephone Number

DATE: 12-08-2005
CLASSIFIED BY 65179 DHM/BAW/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-08-2030

CA# 05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

[redacted] OGC) (FBI)

From: [redacted] (OGC) (FBI) b6 b7C
Sent: Monday, July 19, 2004 11:47 AM
To: [redacted] (OGC) (FBI)
Subject: FBI reposnses to congressional inquiries.

b1 b6 b7C

~~SECRET~~
RECOR [redacted] (S)

[redacted] the anwer to question 103 is out of date. I had sent you the enclosed email to reflect that the answer needed to be changed, based on the fact that in fact the business record order was served and [redacted] was produced.

[redacted]

-----Original Message-----
From [redacted] (OGC) (FBI)
Sent: Tuesday, July 06, 2004 3:05 PM
To [redacted] (OGC) (FBI) b1 b6 b7C
Subject: RE: FISC ORDER

~~SECRE~~
RECOR [redacted] (S)

[redacted] per my earlier email that had responses to questions 60,90, and 103, I need to amend the answer to 103 (b) since I just got updated information as to the service of the first business record order. The response should read:

[redacted] S)

[redacted] b1 , b2, b2, b5, b6, b7C, b7E

-----Original Message-----
From [redacted] (AL) (FBI)
Sent: Tuesday, July 06, 2004 2:35 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (WF) (FBI)
Subject: FISC ORDER

b1 ,b2, b5, b6, b7C, b7E

~~SECRET~~
RECOR [redacted] (S)

[redacted] (S)

~~SECRET~~

b2
b6
b7C

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations
DECLASSIFICATION EXEMPTION 1
SECRET

SECRET

215 Delegation

[redacted] (OGC) (FBI)

b6
b7C

From: [redacted] OGC) (FBI)
Sent: Wednesday, May 04, 2005 7:55 AM
To: [redacted] OCA) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: RE: Request for Classification Guidance

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

I read the last bullet in the attached wpd and do not see that it raises any classification issues. The bullet does not provide any information that [redacted] as concerned about. I defer to WFO regarding any operational concerns vis-a-vis their pending case. [redacted]

-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Tuesday, May 03, 2005 3:16 PM
To: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: Request for Classification Guidance

b6
b7C

UNCLASSIFIED
NON-RECORD

Willie Hulon is testifying on Thurs (5/5) before the House Judicary Crime Subcommittee re Patriot Act §212 (emergency disclosures by ISPs). In prepping him for this hearing, we obtained reports from TLU relating to use of §212. The attached wpd are bullets summarizing the reports that were prepared for Mr. Hulon.

Between Jan and March 2003 there was a spike in the use of §212 that is attributed to a particular investigative effort that is described in the WFO e-mail that is also attached. [redacted] Mr. Hulon [redacted]

[redacted] b5

Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI)

From: [redacted](OGC) (FBI) b6
Sent: Friday, April 01, 2005 10:45 AM b7C
To: [redacted]OGC) (FBI)
Cc: [redacted]OCA) (FBI)
Subject: FW: ISO Details

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

[redacted] Any ideas? b6
b7C
-----Original Message-----
From [redacted](OCA) (FBI)
Sent: Friday, April 01, 2005 10:35 AM
To [redacted](OGC) (FBI); [redacted](OGC) (FBI) [redacted](CTD) (FBI); [redacted](CTD) (FBI) [redacted](AL) (FBI)
Subject: ISO Details

b6
b7C

UNCLASSIFIED
NON-RECORD

Last year, FBI OGC (specifically [redacted] of ILU) began drafting a report concerning use of Patriot Act provisions. [redacted] is out of the office on AL this week. The narrative case example was in the earliest versions of the report as an example of information sharing (§203), however, in [redacted] I have not been able to locate any back-up documents that would provide additional details (i.e. subject name) re this case. I'm casting a wide net in the hopes that this narrative rings a bell with someone who could point me in the direction of additional details. Any guidance addressees can provide would be appreciated. Thanks,

[redacted] I've included you because this draft report has been around for a while and may have come through the ExecStaff while you were there.)
b6
b7C

****

In the aftermath of the September 11th attacks, a reliable intelligence asset identified a naturalized U.S. citizen from a middle-eastern country as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. [redacted]

[redacted]

b5

[redacted]
Office of Congressional Affairs

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OGC) (FBI)

b6

From: [redacted] (OGC) (FBI) b7C

Sent: Tuesday, November 16, 2004 7:12 AM

To: [redacted] TD) (FBI) [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)

Subject: RE: 207208 letter

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-23-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

UNCLASSIFIED
NON-RECORD

Agree.

b6
b7C

-----Original Message-----
From: [redacted] (ITD) (FBI)
Sent: Monday, November 15, 2004 8:05 PM
To: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Cc: [redacted] (ITD) (FBI)
Subject: RE: 207208 letter

UNCLASSIFIED
NON-RECORD

Unless I hear back otherwise, given everyone's comments, I will reply back to the USAO that FBI OGC is reviewing the matter and that they should inform the local FBI agents that they should not send out the letter without first conferring with FBI OGC NSLB.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]
Associate General Counsel - Unit Chief
Science & Technology Law Unit
Engineering Research Facility
[redacted]

b2
b6
b7C

b6
b7C

-----Original Message-----
From [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 11:43 AM
To [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI) [redacted] (ITD) (FBI)
Subject: RE: 207208 letter

UNCLASSIFIED
NON-RECORD

Since the pony [redacted] ent refers to ITOS II, let me see what I can find out from my end.

b6
b7C

CA# 05-CV-0845

[redacted] (OGC) (FBI)

From: [redacted] OGC) (FBI) b6 b7C
Sent: Wednesday, August 25, 2004 10:44 AM
To: [redacted] (OCA) (FBI)
Cc: [redacted] (OCA) (FBI) [redacted] (OGC) (FBI)
Subject: RE: Classified Input re Patriot Act cases

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

UNCLASSIFIED
NON-RECORD

[redacted] On tracking Patriot Act sunset provisions, ILU made that suggestion early on--and I don't know where it went--but it was not done. We have since scrubbed the field--via CDCs for input and I know that NSLB has done the same with CTD but, We can't make anybody do anything--all we can do is ask and thankfully, most CDCs are conscientious enough to help out but all they can at the FO level is ask as well. [Also, I know that EOUSA surveyed US Attorney's offices but, again, a response was not mandatory by them either and the responses reflect that]. In my opinion, the only way to ensure responsiveness, completeness, accuracy, and timeliness is for our front office to mandate reporting of incidents. b6 b7C

-----Original Message-----
From [redacted] (OCA) (FBI)
Sent: Tuesday, August 24, 2004 6:56 PM
To [redacted] (OGC) (FBI) b6 b7C
Cc [redacted] (OCA) (FBI) [redacted] (OGC) (FBI)
Subject: RE: Classified Input re Patriot Act cases

UNCLASSIFIED
NON-RECORD

[redacted] - generally I think the meeting went o.k. [redacted]

[redacted] b6 b7C

Patriot Act will continue to be scrutinized - even beyond the sunset. If you or [redacted] have any thoughts on how we can accomplish this, I'd appreciate it.

Also [redacted] - on the Senate Ethics Committee request - DOJ advised this afternoon that [redacted] - I'll keep you posted. Thanks,

b2 b5 b6 b7C

[redacted]
Office of Congressional Affairs
[redacted]

-----Original Message-----
From [redacted] (OGC) (FBI) b2 b6 b7C
Sent: Tuesday, August 24, 2004 4:29 PM
To: [redacted] OCA) (FBI)

Cc: [redacted](OCA) (FBI); [redacted](OGC) (FBI)
Subject: RE: Classified Input re Patriot Act cases

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] how did this meeting turn out?

b6
b7C

-----Original Message-----
From: [redacted](OCA) (FBI)
Sent: Monday, August 23, 2004 6:23 PM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Cc: [redacted](OCA) (FBI)
Subject: RE: Classified Input re Patriot Act cases

UNCLASSIFIED
NON-RECORD

[redacted] and I spoke. We're happy to staff this meeting and report back - I think that OLP is going to suggest that we go back to the drawing board and [redacted] and I are happy to defend our methodology in collecting the info and advocate for getting something to CMS, even if DOJ thinks we can get better examples if we ask differently. You're welcome to send someone if you want to - or we'll report back. Thanks,

b6
b7C

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, August 23, 2004 1:05 PM
To: [redacted](OGC) (FBI); [redacted](OCA) (FBI)
Cc: [redacted](OCA) (FBI)
Subject: RE: Classified Input re Patriot Act cases

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] I have an 11:00 am meeting and [redacted] who helped on this is out of the office until Wednesday. Spike is out as well until Wednesday. I'll see if I can get someone else to go. [redacted]

b6
b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, August 23, 2004 12:26 PM
To: [redacted](OCA) (FBI)
Cc: [redacted](OCA) (FBI); [redacted](OGC) (FBI)
Subject: RE: Classified Input re Patriot Act cases

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] Not sure I could contribute much to a discussion of the classified portion

of the sunset provisions. Although we put the whole thing together, the classified parts are CTD/NSLB input. But, I can go if you want.

-----Original Message-----
From: [redacted] OCA) (FBI) b6 b7C
Sent: Monday, August 23, 2004 12:22 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OCA) (FBI)
Subject: FW: Classified Input re Patriot Act cases

UNCLASSIFIED
NON-RECORD

DOJ has scheduled at meeting tomorrow at 10:30 am in the OIPR conference room (6150 main) to discuss our classified report re Patriot Act sunset provisions. [redacted] b2 b5
[redacted] While I'm not sure that deadline is firm, I believe we have a considerable interest in getting DOJ to sign off on our draft. b6
I am planning to attend, as is [redacted] Please advise if you can attend or send a designee. Thanks, b7C

[redacted]
Office of Congressional Affairs b6
[redacted] b7C

-----Original Message-----
From: [redacted] (OGC) (OGA)
Sent: Monday, August 23, 2004 11:58 AM
To: [redacted] OCA) (FBI)
Subject: RE: Classified Input re Patriot Act cases

UNCLASSIFIED
NON-RECORD

OK, looks like 10:30 works for us over here. As of right now, it will be OLA (Sean McLaughlin and Dave Blake), OLP (Rachel Brand), OIPR [redacted] and possibly representatives from ODAG, CRM and/or EOUSA. We will meet in the OIPR conference room (6150 main). b6 b7C

-----Original Message-----
From: [redacted] OCA) (FBI) b6
Sent: Monday, August 23, 2004 11:19 AM b7C
To: [redacted] (OGC) (OGA)
Subject: RE: Classified Input re Patriot Act cases

UNCLASSIFIED
NON-RECORD

10:30 tomorrow is great for me! Thanks,

[redacted] b6 b7C

Office of Congressional Affairs
[redacted]

b2
b6
b7C

-----Original Message-----
From [redacted] (OGC) (OGA)
Sent: Monday, August 23, 2004 11:14 AM
To: [redacted] OCA) (FBI)
Subject: RE: Classified Input re Patriot Act cases

UNCLASSIFIED
NON-RECORD

Is tomorrow at 10:30am a good time for your to meet on this? I'll probably invite OLA/OLP/OIPR and possibly ODAG.

-----Original Message-----
From: [redacted] OCA) (FBI)
Sent: Monday, August 23, 2004 10:44 AM
To: [redacted] (OGC) (OGA)
Cc: [redacted] (OGC) (FBI); [redacted] (OCA) (FBI)
Subject: Classified Input re Patriot Act cases
Importance: High

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] I got a call this morning fro[redacted] General Counsel's office) asking about the status of the FBI's input into the classified IC report on Patriot Act cases. When I spoke with [redacted] about this last week (I think you know [redacted] started a detail at Senate Judiciary last week), he said it was at DOJ?
Is that correct and do you have any info re when the review will be complete?
[redacted] offered this morning that [redacted] is anxious to get this out and may finalize the response without FBI/DOJ input.

(S)
(S)
(S)

b1
b2
b6
b7C

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6 b7C
Sent: Sunday, August 08, 2004 9:40 AM
To: [redacted] (OGC) (FBI) CA# 05-CV-0845
Subject: RE: CTD responses

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] Section 203 of the Patriot Act has nothing to do with FISA. It permits the sharing of Title III information - I explained this t[redacted]ast week. I am at a loss on how to get this point across to them. Could you please sit down **in person** with [redacted] and/or his unit chiefs and iron this out? [redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, August 06, 2004 4:50 PM
To: [redacted] (OGC) (FBI)
Subject: FW: CTD responses
Importance: High

b6 b7C

DATE: 12-10-2005
CLASSIFIED BY 65179 DMH/BAW/PVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-10-2030

05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Please see answers below.

[redacted]
Assistant General Counsel
National Security Law Branch
Ext [redacted]

-----Original Message-----
From [redacted] CTD) (FBI)
Sent: Friday, August 06, 2004 4:16 PM
To [redacted] OGC) (FBI)
Subject: RE: CTD responses
Importance: High

b6 b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] below are responses to Questions 84 (b), 84 (c) and 90 (e). I apologize for the delay. When last we spoke, I was left with the impression that you were going to reach out to [redacted] the following week. In any event, my Unit Chiefs tried to track down information to respond to the questions. Hopefully, you'll be able to make use of the information. Please feel free to modify/reformat as you see fit. Thanks, and have a good weekend.

b6 b7C

[redacted]
Terrorism Reports and Requirements Section
Counterterrorism Division, FBIHQ, Room 4712
[redacted]

b2 b6 b7C

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

b. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

In regard to the dissemination of Foreign Intelligence Surveillance Act (FISA)-derived electronic, wire and oral intercept information, the FBI's Counterterrorism Division employs a general evaluation and oversight process which includes input from Operational Program Managers, Intelligence Analysts, the National Security Law Branch, and, when necessary, the Department of Justice. The intelligence information's value is assessed for dissemination to not only the Intelligence Community (IC), but also federal, state and local law enforcement entities (dependent upon proposed use, context and nature of any threat-related information), and, when authorized by DOJ, to foreign intelligence services and foreign law enforcement agencies (dependent upon proposed use, context and nature of any threat-related information).

For general FBI intelligence dissemination, minimized FISA-derived intelligence is analyzed and sanitized to protect intelligence sources and methods and, if applicable, United States persons and entities, that may possibly be compromised or negatively impacted if left unprotected. FBI Program Managers and Intelligence Analysts concurrently identify FISA-derived intelligence that is consistent with IC intelligence requirements and interests. This information is subsequently disseminated via an Intelligence Information Report (IIR), an electronic communication format that is widely accepted among the IC as the standard intelligence dissemination vehicle. IIRs consist of raw intelligence, (intelligence which is not finally evaluated), as well as some degree of associated clarifying information which puts the raw intelligence into context. IIRs are drafted and prepared by the FBI's cadre of Intelligence Analysts/Reports Officers.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

Yes, the FBI disseminates raw intelligence via the IIR.

(1) If so, how many such reports have been issued?

During the period August, 2002 (the beginning time-frame in which statistical data was collected), through August, 2004, the Counterterrorism Division has disseminated 242 IIRs containing FISA-derived intelligence.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

There are various means by which IIRs are evaluated. Members of the IC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify a means for the customers to contact them directly. IC members will assess the quality/relevancy of the reporting, as well as submit additional collection requirements. Often, IC members forward formal Requests for Information (RFIs) requesting additional information which was protected (not provided) in the IIR (an example would be U.S. Person information). RFIs can provide an excellent indication of intelligence community interest in FBI reporting. The FBI's Office of Intelligence also receives evaluations or assessments of FBI reporting. The Office of Intelligence is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

c. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

The Counterterrorism Division shares foreign intelligence information, as defined in Section 203(d)(2), with the Intelligence Community (IC) through several dissemination

conduits. Dissemination can be through direct classified and unclassified Intelligence Information Reports (IIRs), Intelligence Assessments, Intelligence Bulletins, Teletype Memoranda (TM), or through Intelligence Community websites on a classified network. The FBI also shares intelligence information through membership interaction by IC representatives participating on FBI Joint Terrorism Task Forces (JTTFs) which are operating in 84 locations across the United States. Unclassified, but law enforcement sensitive, intelligence information, also is disseminated to Federal, state, and local law enforcement intelligence components through Law Enforcement Online (LEO), a computer network which provides finished intelligence products, assessments, and bulletins on significant developments or trends.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

Dissemination of Electronic, Wire, and Oral Interception Information to the IC derived through standard criminal procedures may be effected electronically through IIRs, TM, Intelligence Assessments, Intelligence Bulletins. However, dissemination of this intelligence information also may be transacted through the exchange of FBI Letterhead Memoranda (LHMs) among relevant IC members.

(1) If so, how many such reports have been issued?

The FBI has no central database readily to determine the quantity of 203(b)material disseminations through the aforementioned methods.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

There are various means by which IIRs are evaluated. Members of the USIC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify a means for the customers to contact them directly. IC members will assess the quality/relevancy of the reporting, as well as submit additional collection requirements. Often, IC members forward formal Requests for Information (RFIs) requesting additional information which was protected (not provided) in the IIR (an example would

be U.S. Person information). RFIs can provide an excellent indication of IC interest in FBI reporting. The FBI's Office of Intelligence also receives evaluations or assessments of FBI reporting. The Office of Intelligence is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

The Intelligence Information Report (IIR) is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Policy, Defense and Law Enforcement Communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations or sources. Intelligence information acquired pursuant to Section 215 of the USA-Patriot Act could, if deemed appropriate, be disseminated via an IIR. Between August 2002 and August 2004, the FBI has disseminated approximately 3860 terrorism-related IIRs to the Intelligence Community.

(i) If so, how many such reports have been issued?

None of the information contained in the 3860 terrorism-related IIRs disseminated between August 2002 and August 2004 was acquired pursuant to section 215 of the USA-Patriot Act.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Although the FBI has procedures to evaluate the quality of intelligence reports, no reports have been disseminated which contained information obtained via application of section 215.

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Friday, August 06, 2004 10:54 AM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (CTD) (FBI)

b6
b7C

Subject: FW: CTD responses

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C 05-CV-0845

Information regarding question 90. Please let me know if this helps.

Thanks again

[redacted]
Assistant General Counsel
National Security Law Branch b2
[redacted] b6 b7C

-----Original Message-----
From: [redacted] (OGC) (FBI) b1
Sent: Wednesday, August 04, 2004 3:47 PM b2
To: [redacted] OGC) (FBI) b5
Subject: RE: CTD responses b6 b7C b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Yes, there has only beer[redacted] business record order issued, althoug[redacted] more are likely to be filed with the FISC on Friday. As to the intelligence reports, I have no idea what those are, as I've told [redacted] (S)
But they certainly are not a vehicle to transmit information obtained from business record orders - th[redacted] and it was given to the field that needed it and they'd have no reason to transmit it to any other place.

[redacted]

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, August 04, 2004 3:41 PM b6
To: [redacted] (OGC) (FBI) b7C
Subject: FW: CTD responses

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]
[redacted] and I are seeking your knowledge on question # 90 below. b6 b7C

Please see attached emails.

Thank you.

[redacted]
Assistant General Counsel b2
National Security Law Branch b6
[redacted] b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, August 04, 2004 2:53 PM
To: [redacted] OGC) (FBI)
Subject: RE: CTD responses

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Clear this with [redacted] to make sure what I said was correct - we have only obtained [redacted] (S)
business record order. Thanks.

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Wednesday, August 04, 2004 2:50 PM
To: [redacted] (OGC) (FBI)
Subject: FW: CTD responses

b6
b7C

b1
b2
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

FYI.

Interesting information re. question 90.

-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Wednesday, August 04, 2004 2:22 PM
To: [redacted] (OGC) (FBI)
Subject: CTD responses

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I met with [redacted] yesterday and she provided me the full text questions to
b6 which you needed responses. You may recall that [redacted] information did not
b7C reflect the questions accurately or distinguish between the different sections in the Patriot Act. With that being said, I'm coordinating with our Operational Counterparts to try to get appropriate responses. I should have all the responses in by tomorrow morning.

One question which we probably will be unable to answer positively is question 90. This question has to do with Section 215 of the Patriot Act (Tangible items). During
b1 my discussion with [redacted] she recalled onl[redacted]nstance wherein that particular (S)
b2 section was utilized, [redacted] I can't seem to
b5 identify anyone who has knowledge of this incident or, in fact, if there were any other
b6 applications (which is unlikely) of Section 215. This may require a canvass to all field
b7C CDCs. I'm quite sure that CTD [redacted] That's not to say that
b7E we didn't [redacted] although I can't even say that), but the question specifically asks about intelligence reports.

[redacted]
b2
Terrorism Reports and Requirements Section b6
Counterterrorism Division, FBIHQ, Room 4712 b7C
[redacted]

~~SECRET~~

Question 90 states:

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

[redacted]
Assistant General Counsel
National Security Law Branch
[redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI)

DATE: 12-10-2005
CLASSIFIED BY 65179 DMH/BAWPVR
REASON: 1.4 (C)
DECLASSIFY ON: 12-10-2030

From: [redacted] (OGC) (FBI) b6 b7C
Sent: Wednesday, August 04, 2004 2:53 PM
To: [redacted] (OGC) (FBI)
Subject: RE: CTD responses

CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Clear this with [redacted] to make sure what I said was correct - we have only obtain[redacted] usiness record order. (S)
Thanks.

b1
b2
b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-24-2005 BY 65179 DMH/CLS

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Wednesday, August 04, 2004 2:50 PM
To: [redacted] OGC) (FBI)
Subject: FW: CTD responses

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

FYI.

Interesting information re. question 90.

[redacted] b2
Assistant General Counsel b6
National Security Law Branch b7C
[redacted]

-----Original Message-----
From [redacted] (CTD) (FBI)
Sent: Wednesday, August 04, 2004 2:22 PM
To: [redacted] OGC) (FBI)
Subject: CTD responses

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] I met with [redacted] esterday and she provided me the full text questions to which you needed responses. You may recall that [redacted] information did not reflect the questions accurately or distinguish between the different sections in the Patriot Act. With that being said, I'm coordinating with our Operational Counterparts to try to get appropriate responses. I should have all the responses in by tomorrow morning.

b1
b2
b5
b6
b7C
b7E

One question which we probably will be unable to answer positively is question 90. This question has to do with Section 215 of the Patriot Act (Tangible items). During my discussion with [redacted] she recalled only [S] [redacted] nstance wherein that particular section was utilized, [redacted] I can't seem to identify anyone who has knowledge of this incident or, in fact, if there were any other applications (which is unlikely) of Section 215. This may require a canvass to all field CDCs. I'm quite sure that CTD [redacted] That's not to say that we didn't [redacted] (although I can't even say that), but the question specifically asks about intelligence reports.

[redacted]
Terrorism Reports and Requirements Section
Counterterrorism Division, FBIHQ, Room 4712
[redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SECRET

[redacted](OGC) (FBI)

From: [redacted](OGC) (FBI) b6
Sent: Tuesday, August 03, 2004 3:41 PM b7C
To: [redacted](CTD) (FBI)
Subject: FW: NSLB Responses - Secret [OGC seeking assistance from CTD]
Importance: High

(U)

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

CA# 05-CV-0845

-----Original Message-----
From: [redacted](OGC) (FBI) b6
Sent: Tuesday, August 03, 2004 11:34 AM b7C
To: [redacted](CTD) (FBI)
Cc: [redacted](OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI)
Subject: FW: NSLB Responses - Secret [OGC seeking assistance from CTD]
Importance: High

(U)

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] OGC was tasked with answering certain QFRs from the Director's testimony in May. Some require assistance from CTD. Approximately 2 or so weeks ago we contacted [redacted] who graciously agreed to help. The task is now assigned to [redacted] We have left several reminders with [redacted] but have not received a response. I know he is probably very busy but OCA is pushing us to get the answers finalized. Could you help us? Thanks [redacted]

-----Original Message-----
From: [redacted](OGC) (FBI) b6
Sent: Tuesday, August 03, 2004 11:17 AM b7C
To: [redacted](OGC) (FBI)
Subject: FW: NSLB Responses - Secret [OGC seeking assistance from CTD]
Importance: High

(U)

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

Here is the whole string of emails. Hopefully you can make sense of it. b2 b6 b7C

[redacted]
Assistant General Counsel
National Security Law Branch
[redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, July 23, 2004 2:43 PM
To: [redacted](CTD) (FBI)
Subject: FW: NSLB Responses - Secret [OGC seeking assistance from CTD]
Importance: High

(U)

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I just received an Outlook Auto response that [redacted] s out of the office today and possibly Monday. OGC is trying to respond to OCA by COB today.

Would you be able to address the following issues (please see emails below).

Any help would be greatly appreciated.

Thank you in advance,

[redacted]
Assistant General Counsel
National Security Law Branch
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Friday, July 23, 2004 2:39 PM
To: [redacted] (CTD) (OGA)
Subject: FW: NSLB Responses - Secret [OGC seeking assistance from CTD]
Importance: High

(U)

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Thank you for your previous help with the questions from OCA. As indicated in my previous email, we unfortunately need more specific answers to the three questions that you so generously provided earlier.

I am sure that you are extremely busy, but OCA is looking for a response no later than COB today. Therefore, any help would be greatly appreciated.

In addition, we wanted to make sure that CTD agrees with our answer to Question 89d, where we state in our response to refer to question 85.

89d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

Please let me know if any of this is possible.

Thank you in advance. Please do not hesitate to contact me for any reason.

[redacted]

Assistant General Counsel
National Security Law Branch
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: [redacted] 21, 2004 2:41 PM
To: [redacted] (CTD) (OGA)
Subject: RE: NSLB Responses - Secret (U)

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

Thank you for your responses. Unfortunately, we still have some follow up questions. Question 84 (b) is specific to section 203 (b) which deals with disclosure to grand jury, title 3 etc. Question 84 (d) specifically deals with Section 203 (d) and question 90(e) deals with Section 215 (business records, etc.) of the USA-Patriot Act.

Is it possible to obtain anything more specific?

I appreciate all the help that you have provided with this, and as always any additional information is greatly appreciated.

Please note that I have attached the selected questions to this email.

If you have any questions, please do not hesitate to contact me.

Again, thank you.

[redacted]

Assistant General Counsel
National Security Law Branch
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (CTD) (OGA)
Sent: Tuesday, July 20, 2004 9:19 AM
To: [redacted] OGC) (FBI)
Cc: [redacted] (CTD) (FBI); [redacted] (CTD) (FBI)
Subject: RE: NSLB Responses - Secret (U)

UNCLASSIFIED

[redacted]

[redacted]

b5

-----Original Message-----
From [redacted] OGC) (FBI) b6
Sent: Monday, July 19, 2004 4:34 PM b7C
To [redacted] (CTD) (OGA)
Subject: FW: NSLB Responses - Secret (U)
Importance: High

UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

I just left you a message regarding this issue.

NSLB is seeking assistance with three questions posed by OPA/OCA. [redacted] said you are the person with the answers.

NSLB supplied the following attached answers to OPA/OCA. We incorporated the answer that you supplied to question 85. There are three other answers that we thought CTD would be able to answer better/more complete than OGC and indicated such in OGC's responses. (Response to questions 84(b), 84(c), and 90 (e)). We believe that portions of the responses can be found in the answer to 85 that you previously supplied.

OCA stated that they would not accept OGC's answers to 84(b), 84(c), and 90 (e)

and that we needed to contact CTD for the answers.

Please let me know if this is possible. Any help is greatly appreciated.

[redacted]
Assistant General Counsel
National Security Law Branch
Ext. [redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Monday, July 19, 2004 2:50 PM
To [redacted] (OGC) (FBI)
Subject: NSLB Responses - Secret (U)

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, July 29, 2004 5:38 PM
To: [redacted] (OGC) (FBI) [redacted] OGC) (FBI)
Cc: [redacted] (OI) (FBI) [redacted] (OGC) (FBI)
Subject: TIDE (TTIC) Information Sharing

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b5

[redacted]

[redacted]
Office of the General Counsel
[redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Monday, July 26, 2004 10:22 AM b7C
To: [redacted] (OGC) (FBI)
Subject: FW: Sunset provisions

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

Here it is.
-----Original Message-----
From: [redacted] (OGC) (FBI) b6
Sent: Tuesday, July 20, 2004 12:20 PM b7C
To: [redacted] (OCA) (FBI)
Cc: BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (OGA); [redacted] (OCA) (FBI)
Subject: Sunset provisions

~~SECRET~~//ORCON,NOFORN
RECORD 66F-HQ-C1364260

[redacted] attached are our comments and the results of our field and HQ survey on the Patriot Act sunset provisions. We folded in the examples provided by NSLB so it is one complete OGC package. [redacted] kept the classification she received for the examples but she deleted most of the references to subject's names, locations,etc--so I am sure that much what is labled SECRET can be declassified--but I can't do that, which is why I copied Spike. b6 b7C

Not knowing what format you wanted, I just sent it as is. DGC Pat Kelley has approved it as well.

[redacted] b2
Office of the General Counsel b6
[redacted] b7C

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFY ON: 20140720~~
~~SECRET~~//ORCON,NOFORN

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFY ON: 20140720~~
~~SECRET~~//ORCON,NOFORN

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Friday, July 23, 2004 10:04 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: Patriot Act 203(d) Issue

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

When last we met, I was going to explore teeing up the question of whether Section 203 (d) trumped two statutory restrictions on sharing foreign intel information from criminal investigations with the IC--NICS information on attempted gun purchases and taxpayer return information.

[redacted] b5

[redacted] b5

[redacted] b5

[redacted]
Office of the General Counsel
[redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

[redacted](OGC) (FBI) b6 b7C

From: [redacted](OGC) (FBI)
Sent: Wednesday, July 21, 2004 5:40 PM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](ITD) (FBI)
Subject: FW: QFRs #104

~~SECRET~~
RECORD 66F-

CA# 05-CV-0845

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Wednesday, July 21, 2004 2:02 PM
To: [redacted](OGC) (FBI)
Subject: FW: QFRs #104

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~
RECORD 66F-

DATE: 12-29-2005
CLASSIFIED BY 65179dmh/BAw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-29-2030

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Tuesday, July 20, 2004 6:55 PM
To: BOWMAN, MARION E. (OGC) (FBI)
Subject: RE: QFRs #104

b6
b7C

~~SECRET~~
RECORD 66F-

Spike,

I took a shot at this, then decided I was being too confrontational to send it, so I'm passing on back to you as a "draft." In addition, I don't know how, in timely fashion, answer the first part without the specifics, which are secret.

[redacted] b6 b7C

TEXT:

Several factors make the proposed requirement unnecessary.

First, the way "roving wiretaps" are provided for by FISA makes them uncommon in real-world application. That is, the FBI can obtain an order for a roving FISA wiretap only under circumstances in which we can show that the target of the proposed surveillance is doing something to make it difficult, if not impossible, to identify the carrier on whom an order may be served. As a matter of fact, this means roving FISA wiretaps are rare. Codifying a requirement is not gong to impact a significant number of instances of electronic surveillance. That is to say, the optics of enacting such legislation may appear to protect innocent Americans from the FBI, but in reality it isn't going to apply to many surveillances at all.

[redacted] [S] b1 b5

[redacted] [S] b1 b5

(S) (U)

The fact of the matter is that we already comply with a requirement that we determine whether the target of a wiretap is present, and legislating that rule would be carrying coals to Newcastle. As a matter of fact, the situation that arises more frequently in the real world is that the FBI is required to forego retention and use of information that really is foreign intelligence information [redacted] (S)

b2 b5 b7E

In my experience, we have never obtained an order to wiretap a target we could not identify if we could not identify the premises to be surveilled, and I am having a difficult time imagining how we could satisfy the statutory requirements for a FISA order without showing PC to believe one or the other. I simply cannot see how we cold make the necessary showing that the target was taking steps to obscure the carrier on whom to serve the order if, not knowing his identity, we could not specify the premises he was using.

-----Original Message-----
From [redacted] CTD) (FBI) b6
Sent: Tuesday, July 20, 2004 2:39 PM b7C
To: BOWMAN, MARION E. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: QFRs #104

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hello,

On 05/20/04 the Director testified before the Senate Judiciary, which has resulted in 270 QFRs to the FBI. Attached you will find one regarding your program. Can you have someone prepare an unclassified response to this question and get it back to [redacted] and myself by 07/22/04. Unfortunately, the deadline is immediate as this question was inadvertently left of the series of questions due to OCA on July 19th. b6 b7C

Below is questions #104.

104. CTD. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

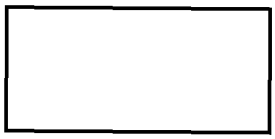
a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518(11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

b. The SAFE Act would also require the FBI to identify either the target of the wiretap or the place to be wiretapped. [redacted] This is a sensible requirement to protect innocent Americans who are not the target of an investigation, b2 b5 b7E

SECRET

while still allowing the FBI to conduct surveillance of suspected terrorists or spies. Why shouldn't Congress enact this prudent safeguard? Please explain.

Thanks,



b2
b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

SECRET

[redacted] (OGC) (FBI)

From: [redacted] (OCA) (FBI) b6
Sent: Wednesday, July 21, 2004 7:13 PM b7C
To: [redacted] (ITD) (FBI) [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: QFRs #104

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] b6 b7C

Can we chat on Thursday? I've tried to put this information together with the question, and I'm confused because it seems like they are trying to MAKE presence of the target a requirement. I'm sure you can explain it to me. Can we talk?

[redacted] b2 b6
Office of Congressional Affairs b7C
JEH Building Room 7252
[redacted]

-----Original Message----- b6
From: [redacted] (ITD) (FBI) b7C
Sent: Wednesday, July 21, 2004 4:32 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: QFRs #104

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Q #85 on roving wiretaps did not present this issue, thus the response [redacted] prepared for Q #85 did not address the issue presented in Q# 104. Might OCA already have sought and obtained a separate response associated with the legislation described: SAFE Act (s 1709) that could be used. For what its worth here's my thoughts: b6 b7C

[redacted] b2 b5 b7E

[redacted] b2 b5 b7E

[redacted] b2 b5 b7E

-----Original Message-----
From [redacted] (OGC) (FBI) b6
Sent: Tuesday, July 20, 2004 4:55 PM b7C
To: [redacted] (ITD) (FBI)
Subject: FW: QFRs #104

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Sorry [redacted] I had the wrong e-mail address in the first e-mail.
-----Original Message----- b6
From [redacted] (OGC) (FBI) b7C
Sent: Tuesday, July 20, 2004 4:44 PM
To [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] OGC) (FBI)
Cc: Curran, John F. (OGC) (OGA); BOWMAN, MARION E. (OGC) (FBI)
Subject: FW: QFRs #104 b2 b6 b7C b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Help!! It appears that QFR #104 was assigned to the Office of Intelligence and they are referring it to us. The question has to do with imposing statutory safeguards on our use of roving wiretaps. [redacted] answered a roving wiretap QFR and that is why I am forwarding this e-mail to them. However [redacted] will be out of the office tomorrow so [redacted] offered up [redacted] to assist. I am forwarding this to [redacted] because I believe the FISA rovings have mainly been used in [redacted] cases so whatever thoughts [redacted] could add would be great. Sorry for the short notice. We just received this request. Thanks.
-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Tuesday, July 20, 2004 4:32 PM b6
To: [redacted] (OGC) (FBI) b7C
Subject: RE: QFRs #104

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Yes, I guess so

-----Original Message-----
From: [redacted] (OGC) (FBI) b6
Sent: Tuesday, July 20, 2004 4:30 PM b7C
To: BOWMAN, MARION E. (OGC) (FBI)
Subject: RE: QFRs #104

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

It was not assigned to anyone in OGC. Do you want us to handle it?

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Tuesday, July 20, 2004 4:13 PM
To: [redacted] (OGC) (FBI)
Subject: FW: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Did we or ILU handle a related question?
-----Original Message-----
From: [redacted] (CTD) (FBI)
Sent: Tuesday, July 20, 2004 2:39 PM
To: BOWMAN, MARION E. (OGC) (FBI); [redacted] OGC) (FBI)
Subject: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hello,

On 05/20/04 the Director testified before the Senate Judiciary, which has resulted in 270 QFRs to the FBI. Attached you will find one regarding your program. Can you have someone prepare an unclassified response to this question and get it back to [redacted] and myself by 07/22/04. Unfortunately, the deadline is immediate as this question was inadvertently left of the series of questions due to OCA on July 19th.

b6
b7C

Below is questions #104.

104. CTD. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518(11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

b. The SAFE Act would also require the FBI to identify either the target of the wiretap or the place to be wiretapped. [redacted] This is a sensible requirement to protect innocent Americans who are not the target of an investigation, while still allowing the FBI to conduct surveillance of suspected terrorists or spies. Why shouldn't Congress enact this prudent safeguard? Please explain.

b2
b5
b7E

Thanks,

[redacted]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

LAMMERT, ELAINE N. (OGC) (FBI)

b6
b7C

From: (OGC) (FBI)
Sent: Tuesday, July 20, 2004 5:00 PM
To: (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI)
Cc: BOWMAN, MARION E. (OGC) (FBI); OGC) (FBI)
Subject: RE: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Listen nd I have not been involved in any roving wiretaps, and are going to be not very helpful here.

b2
b5
b7E

b5

We are different because we are collecting intelligence to prevent a horrible occurence. We are not just collecting evidence. We won't know where the target will be or where they will go.

have you seen a roving FISA?

b6
b7C

-----Original Message-----
From: (OGC) (FBI)
Sent: Tuesday, July 20, 2004 4:44 PM
To: (OGC) (FBI); OGC) (FBI); (OGC) (FBI); (OGC) (FBI); OGC) (FBI)
Cc: Curran, John F. (OGC) (OGA); BOWMAN, MARION E. (OGC) (FBI)
Subject: FW: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Help!! It appears that QFR #104 was assigned to the Office of Intelligence and they are referring it to us. The question has to do with imposing statutory safeguards on our use of roving wiretaps. answered a roving wiretap QFR and that is why I am forwarding this e-mail to them. However, will be out of the office tomorrow so offered up to assist. I am forwarding this to because I believe the FISA rovings have mainly been used in cases so whatever thoughts ould add would be great. Sorry for the short notice. We just received this request. Thanks.

b2
b6
b7C
b7E

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Tuesday, July 20, 2004 4:32 PM
To: (OGC) (FBI)
Subject: RE: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Yes, I guess so

-----Original Message-----
From [redacted](OGC) (FBI)
Sent: Tuesday, July 20, 2004 4:30 PM
To: BOWMAN, MARION E. (OGC) (FBI)
Subject: RE: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

It was not assigned to anyone in OGC. Do you want us to handle it?

-----Original Message-----
From: BOWMAN, MARION E. (OGC) (FBI)
Sent: Tuesday, July 20, 2004 4:13 PM
To: [redacted](OGC) (FBI)
Subject: FW: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Did we or ILU handle a related question?

-----Original Message-----
From: [redacted](CTD) (FBI)
Sent: Tuesday, July 20, 2004 2:39 PM
To: BOWMAN, MARION E. (OGC) (FBI) [redacted](OGC) (FBI)
Subject: QFRs #104

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hello,

On 05/20/04 the Director testified before the Senate Judiciary, which has resulted in 270 QFRs to the FBI. Attached you will find one regarding your program. Can you have someone prepare an unclassified response to this question and get it back to [redacted] and myself by 07/22/04. Unfortunately, the deadline is immediate as this question was inadvertently left of the series of questions due to OCA on July 19th.

b6
b7C

Below is questions #104.

104. CTD. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518 (11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

b. The SAFE Act would also require the FBI to identify either the

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6 b7C
Sent: Friday, July 16, 2004 11:56 AM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: CT Survival Guide

~~SECRET~~
RECORD 66F-HQ-A1247863

b2 b6 b7C

[redacted] National Security Law [redacted] OGC, asked me to review for legal sufficiency Section X of the draft "CT Survival Guide," entitled "Patriot Act". My comments follow.

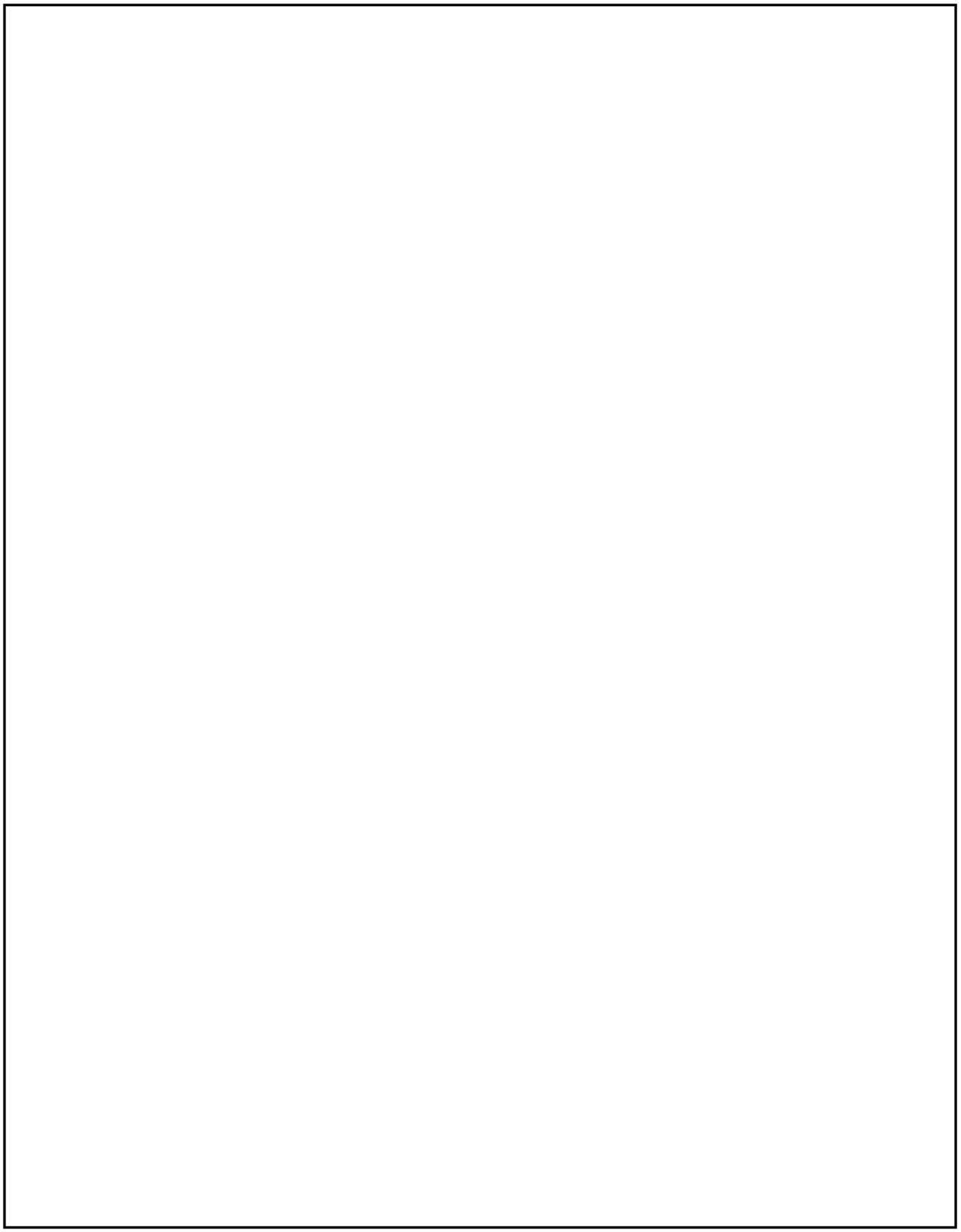
[redacted] b5

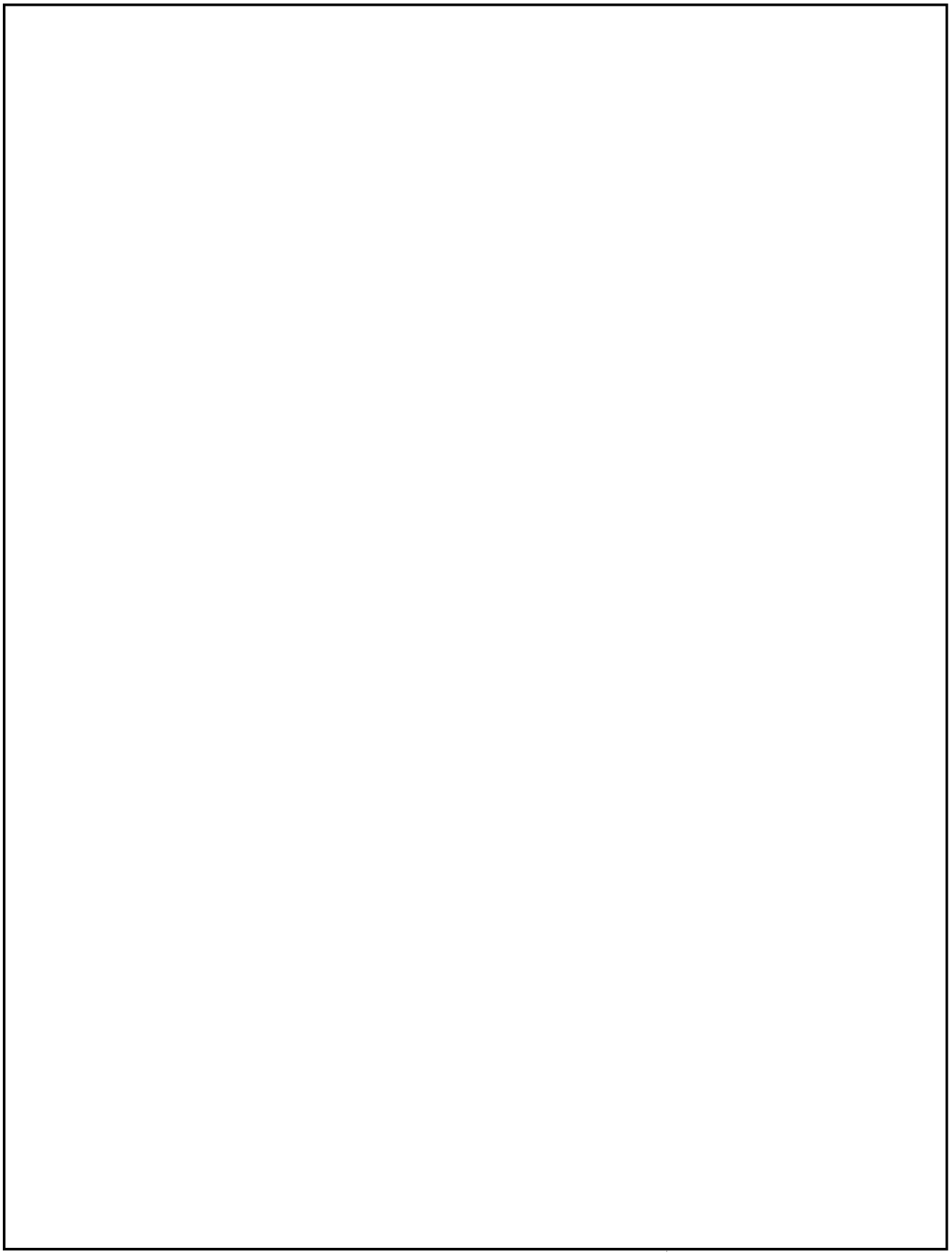
[redacted] b5

[redacted] b5

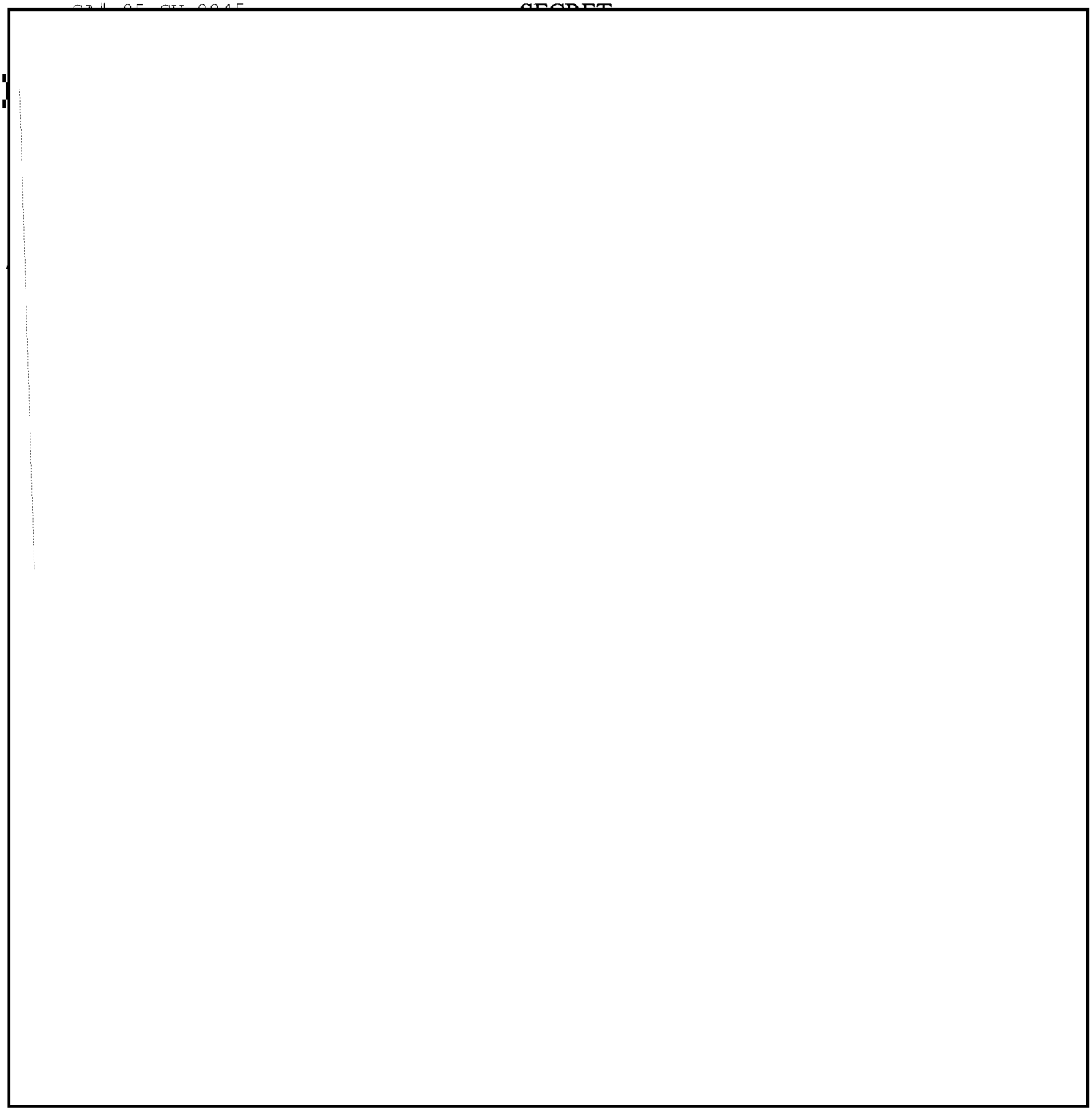
[redacted] b5

[redacted] b5





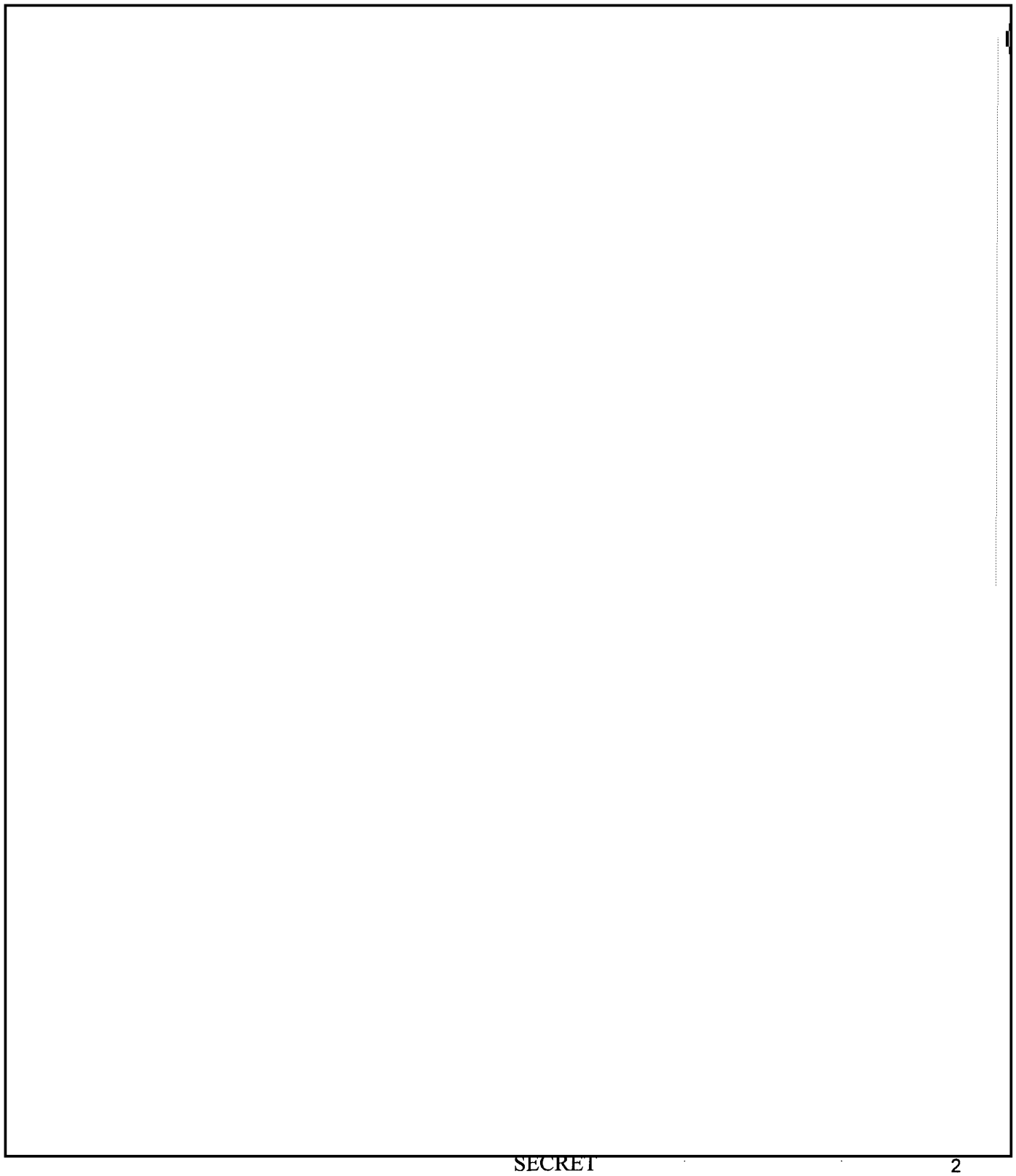
(S)

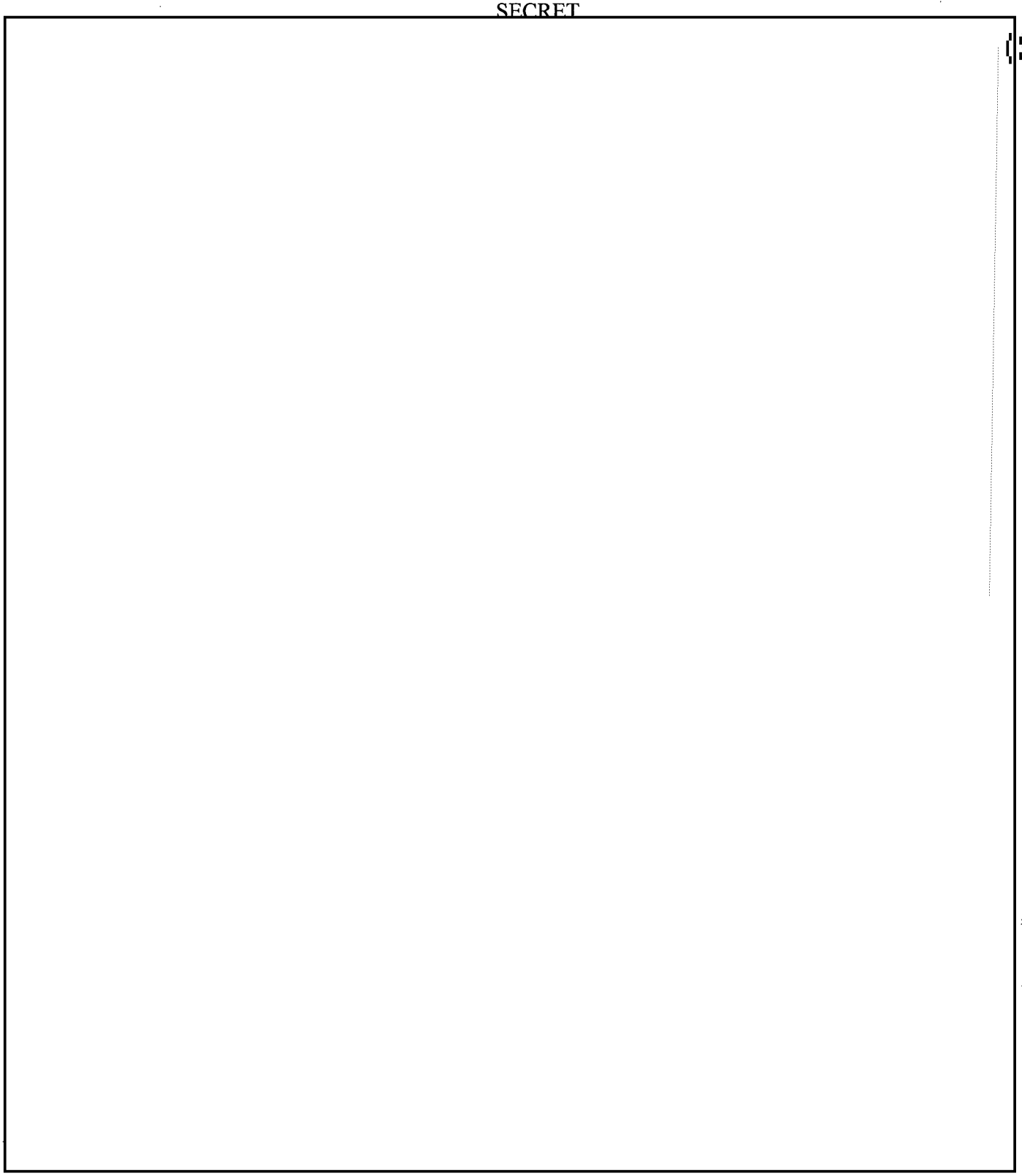


Classified by: 7143, CTD
Declassify on: X1

b1

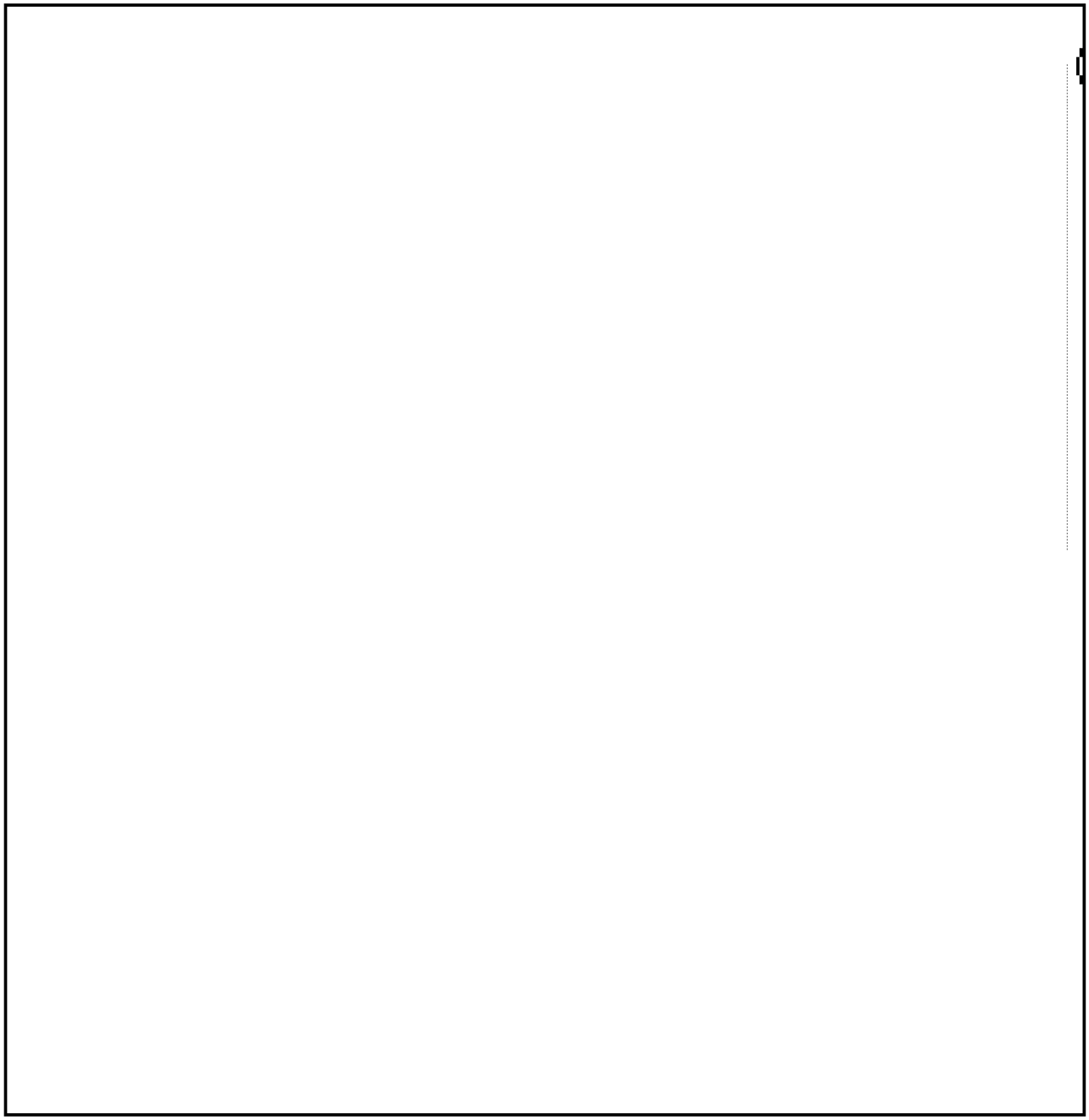
(S)





(S)

- Warrant issued only by Foreign Intelligence Surveillance Court (Attorney General in emergency)
- Ex Parte Order based solely on government's evidence
- Limited Disclosure/Covert Collection



(S)

b1
b2
b5
b7E

[redacted](OGC) (FBI) b6 b7C

From: [redacted] (OGC) (FBI)
Sent: Tuesday, July 13, 2004 1:17 PM
To: [redacted]OGC) (FBI); [redacted]OGC) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: FW: Sunset Provision Examples
Importance: High

~~SECRET~~
RECORD 66F-HQ-C1364260

b6 b7C

[redacted] of ILU needs immediate assistance with a tasking. Senator Feinstein wants to support the Bureau by promoting the renewal of the sunset provisions of the Patriot Act. In order to do so, she needs concrete examples of where the provisions have been useful to specific investigations. CTD provided case summaries but, in most of the cases, it is difficult to ascertain just how the provision(s) was useful to the investigation.

[redacted] and I discussed this tasking and determined that the best and most expedient way of assisting with this would be for the attorneys assigned to the substantive unit with responsibility for the case to review the summary and then meet with the HQ agent to positively determine just how the provision was useful. [redacted] cautioned that many of the agents are unfamiliar with the exact provisions of the Patriot Act. Some do not realize that the provisions used in the investigation derived from the Patriot Act and are destined to go away if not renewed. Thus, you may need to educate the agent about the provisions before discussing with them how they were useful to specific investigations. [redacted] is just looking for a couple of lines. [redacted] note below provides a good explanation.

b6 b7C

From my quick review, it looks like the bulk of these are CONUS II and III cases.

[redacted] SSA [redacted] are listed on many of the summaries. I think [redacted] but of WFO is CONUS II as well.

b6 b7C

[redacted] Many summaries have SSA [redacted] name attached. I think he is CONUS III. SSA [redacted] [redacted] is also listed as is SSA [redacted] (*I think he is CONUS IV but you were kind enough to agree to take this i*[redacted] absence).

b6 b7C

If I am wrong in my assignment to the two of you for all the summaries, please let me know ASAP. Sorry for the short deadline, and thanks. Please see [redacted] message below. Let me know if I can offer any help.

b6 b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Tuesday, July 13, 2004 12:56 PM
To: [redacted](OGC) (FBI)
Subject: Sunset Provision Examples

b6 b7C

~~SECRET~~
RECORD 66F-HQ-C1364260

[redacted] As per our conversation earlier today, I'm soliciting the assistance of NSLB attorneys as they may be more familiar with the terrorism cases than I am. Attached is a list of case summaries submitted by CTD that may be examples of how the various sunset provisions of the Patriot Act were utilized. I have placed them in categories based upon the sunset provision that the field asserts was utilized on that case, however, for most cases it is difficult for me to ascertain how that provision was utilized and if it was helpful in the case.

Could NSLB review the case summaries and talk to anyone in CTD or the field in order to advise me specifically how that provision of the Patriot Act was helpful. The information can be classified. Please provide that information to me either via a phone call TODAY, or via e-mail by COB today. I am under an extremely tight deadline so that a classified list of examples might be provided to Senator Feinstein in an effort to justify the renewal of these provisions.

Attached is both the classified submission by CTD and a brief synopsis of the effect of each provision.

Thank you in advance for your help on this effort!

[redacted]
ILU/OGC
[redacted]

b2
b6
b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

[redacted] (OGC) (FBI) b6

From: [redacted] OGC) (FBI) b7C

Sent: Wednesday, July 07, 2004 4:08 PM

To: [redacted] (CTD) (FBI)

Cc: [redacted] OGC) (FBI); AINORA, THOMAS (OGC) (FBI)

Subject: Legal Review of "On the Job Guidebook"

~~SECRET~~
RECORD 66F-HQ-A1247863

b6
[redacted] b7C

I and several National Security Law Branch attorneys are reviewing assigned portions of your draft "On the Job Guidebook" for legal sufficiency. I assigned myself the chapters on the Foreign Intelligence Surveillance Act and IOBs, which I'll do separately.

[redacted] b5 b6 b7C

Also, in the first paragraph in that section [redacted] b5

Same paragraph: A nit--the word "government" is never capitalized unless it appears with the initials "U.S." The same rule applies to the word "federal." GPO Style Manual.

Same section, third paragraph: [redacted]

Re the next page (p. 27), I believe you have melded your discussions of probable cause and primary purpose without intending to do so. I recommend you break them out as follows: b5

[redacted] b5

In criminal investigations, for years the courts applied a two-pronged test for probable cause. The first prong required police officers to assess the credibility of a source; the second prong required an assessment of the source's basis of knowledge. In a 1983 decision, Illinois vs. Gates (462 U.S. 213) the U.S. Supreme Court reviewed the state of the law to that point and concluded that the correct test for probable cause was a "totality of circumstances" test. While this test requires more than an unfounded suspicion, courts applying the Illinois vs. Gates standard have recognized that probable cause is less demanding than the evidentiary standard of beyond a reasonable doubt and is a lower standard than "preponderance of the evidence." As a result, magistrates reviewing criminal warrants are now simply required "to make a practical, common-sense decision whether, given all the circumstances set forth in [an] affidavit . . . this is a fair probability that . . . evidence of a crime will be found in a particular place." Illinois vs. Gates, 462 U.S. 213 at 238.

FISA has this same legal standard for probable cause: totality of the circumstances. However, unlike criminal cases where a magistrate is looking for specific evidence of a crime, the Foreign Intelligence Surveillance Court

(FISC) will review an Agent's declaration of facts to determine whether probable cause -- i.e., a totality of circumstances -- exists to believe the target of proposed search or surveillance is a "foreign power" or "an agent of a foreign power," as those terms are defined in FISA. Additionally, if the subject of the proposed search or surveillance is a "United States person" as defined in FISA, the FISC must further determine whether probable cause exists to believe the target is engaged in activities that involve or may involve criminal conduct. See 50 U.S.C. § 1801(b). Additionally, for an electronic surveillance or search order to be issued, the FISC must also find that there is probable cause to believe that each of the facilities or places to be searched or surveilled is being used, or about to be used, by an a foreign power or an agent of a foreign power. Thus, while the specific findings of fact are different under FISA, in each instance the underlying legal standard -- i.e., the test for probable cause remains the same: the totality of the circumstances, just as it is in criminal cases."

b5

b5

The USA Patriot Act eliminated the wall entirely. Now, rather than requiring the Director of the FBI and the Attorney General to certify that "the purpose" of a FISA search or surveillance was to obtain foreign intelligence information, it is legally permissible to certify that "a significant purpose" of the FISA is to obtain foreign intelligence information. This change in the law thus eliminates the need for FBI investigators to evaluate whether an investigation has a predominately criminal or intelligence purpose. It no longer matters. The Attorney General has opined that FISA can now be used "primarily for a law enforcement purpose, so long as 'a significant purpose'" is also to obtain foreign intelligence information. This change in the law thus permits the full coordination between intelligence community and law enforcement personnel. This fact is reflected in the current Attorney General Guidelines, which state in part:

> [T[he FBI shall provide intelligence information expeditiously to other agencies in the Intelligence Community so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions." b2 ,b5, b6, b7C, b7E

From there I think you can return to your on page 27. In this regard, to ensure you and I are thinking the same thoughts, in the second full paragraph on p. 27 you indicate that I think you need to be more precise in your choice of words. b5

You describe this process correctly and completely in the next paragraph. I recommend you The rest of that paragraph is legally sufficient as written.

Re the Section titled "Basic FISA Request Content," page 28, He does a lot of your work for you. b5 ,b6, b7C

In the same section, I recommend b5

b5

(OGC) (FBI)

From: (OGC) (FBI) b6 b7C
Sent: Monday, June 07, 2004 11:13 AM
To: (OGC) (FBI)
Subject: RE: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

UNCLASSIFIED
NON-RECORD

b5 b6 b7C

-----Original Message-----
From: (OGC) (FBI) b6 b7C
Sent: Monday, June 07, 2004 11:00 AM
To: (OGC) (FBI); (OGC) (FBI); (OGC) (FBI); (OGC) (FBI)
Cc: BOWMAN, MARION E. (OGC) (FBI)
Subject: FW: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

UNCLASSIFIED
NON-RECORD

I know it is really short notice (I advised OCA that I did not think we could get our comments to them by 11:00 am) but if you have comments please let us know.

-----Original Message-----
From: (OCA) (FBI)
Sent: Monday, June 07, 2004 9:06 AM
To: (OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI); (OGC) (FBI); (CID) (FBI); (CID) (FBI); ANDRESS, BEVERLY (CD) (FBI); (CD) (FBI); RUSSO, ROSANNE (CD) (FBI); (CTD) (FBI); HARRINGTON, T J. (CTD) (FBI); BAGINSKI, MAUREEN A. (DO) (FBI); (DO) (FBI) b6 b7C
Subject: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

UNCLASSIFIED
NON-RECORD

The attached testimony is being given before Congress. Please review the testimony and provide your comments, if any, to CAO. Please indicate if your division is in favor or opposed to the testimony as well as the reasons for your division's position. If your division opposes the testimony fully or in part, but believes that it can be remedied by changes in the verbiage, please describe in detail what should be added, deleted, or changed, including recommendations for substitute language sufficient to correct the objectionable section(s).

Please E-mail your comments to SSA with a cc to Your comments should be prepared in Microsoft Word format which is suitable for dissemination to DOJ and to congressional staff. Please send these comments to the CAO contact person as an b6 b7C

attachment to your E-mail. If you have additional comments which are not suitable for dissemination, please include them in the body of your E-mail separate and apart from the attachment. If your division is not taking a position and has no comments, please send an E-mail to the CAO contact person stating such.

DEADLINE 11:00 am 6-7-04. We appreciate your attention to this matter.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI)

b6

From: [redacted]CA) (FBI) b7C

Sent: Monday, June 07, 2004 9:06 AM

To: [redacted](OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI); [redacted](OGC) (FBI); [redacted](CID) (FBI); [redacted](CID) (FBI); ANDRESS, BEVERLY (CD) (FBI); [redacted](CD) (FBI); RUSSO, ROSANNE (CD) (FBI); [redacted](CTD) (FBI); HARRINGTON, T J. (CTD) (FBI); BAGINSKI, MAUREEN A. (DO) (FBI); [redacted](DO) (FBI)

Subject: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

Follow Up Flag: Follow up

Due By: Monday, June 07, 2004 11:00 AM

Flag Status: Flagged

UNCLASSIFIED
NON-RECORD

The attached testimony is being given before Congress. Please review the testimony and provide your comments, if any, to CAO. Please indicate if your division is in favor or opposed to the testimony as well as the reasons for your division's position. If your division opposes the testimony fully or in part, but believes that it can be remedied by changes in the verbiage, please describe in detail what should be added, deleted, or changed, including recommendations for substitute language sufficient to correct the objectionable section(s).

Please E-mail your comments to SSA [redacted]with a cc to [redacted] Your comments should be prepared in Microsoft Word format which is suitable for dissemination to DOJ and to congressional staff. Please send these comments to the CAO contact person as an attachment to your E-mail. If you have additional comments which are not suitable for dissemination, please include them in the body of your E-mail separate and apart from the attachment. If your division is not taking a position and has no comments, please send an E-mail to the CAO contact person stating such.

b2
b6
b7C

DEADLINE 11:00 am 6-7-04. We appreciate your attention to this matter.

UNCLASSIFIED

[redacted] (OGC) (FBI)

b6 b7C

From: [redacted] (Div00) (FBI)
Sent: Tuesday, May 18, 2004 7:19 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] A. (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] Div09) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

UNCLASSIFIED
NON-RECORD

I spoke with Rachel Brand @ DOJ OLP. She advised as follows:
(S) Delayed Notice - use[redacted]mes - although this is an old number and should be updated. She was not aware that it had been updated. b1 b5
Roving Wiretaps - # is classified
215 Requests - # (0) was declassified in Sept '03, but has not been declassified since. In Rachel's opinion [redacted]

If NSLB has additional data that would be helpful for the Director's background information, it would be appreciated. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2 b6 b7C

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:52 PM
To: [redacted] (Div09) (FBI); [redacted] (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

UNCLASSIFIED
NON-RECORD

[redacted] NSLB will assist you in obtaining the numbers of Roving FISAs and 215 requests As to delay notice [redacted] I would call CTS, OEO or OLP. b5

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 2:03 PM
To: [redacted] (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

b6 b7C

UNCLASSIFIED
NON-RECORD

[redacted] I can provide you the results from the field survey that OGC conducted, however, I can also

guarantee that these are not entirely accurate numbers. The field survey was voluntary, and the level of detail provided varied between the field offices. Furthermore, since then I have been advised that some HQ divisions have been utilizing various Patriot Act tools, and I did not receive any contributions from any HQ division on this survey, so their use is not included in any numbers that I have.

The field offices reported the following:

Section 206 - Roving FISA orders [redacted](S) mes b1
Section 215 - Use[redacted](S) mes[redacted](S) ditional orders currently in approval process b2 b7E
Section 213 - Delayed Notice for Search Warrants - This is not a sunset provision, so we did not seek field input on this specific provision at this time.

Also - as you are aware, field offices collect statistics on their accomplishments (i.e. search warrants executed). I believe that Finance Division maintains, compiles, and reports these statistics. They may have more accurate field wide numbers.

I hope this is helpful.

[redacted] b2
Assistant General Counsel b6
Investigative Law Unit
Office of the General Counsel b7C
[redacted]

-----Original Message-----
From: [redacted] (Div00) (FBI)
Sent: Tuesday, May 18, 2004 1:41 PM
To: BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div00) (FBI) b6
Subject: Statistics re USA PATRIOT Act provisions b7C
Importance: High

UNCLASSIFIED
NON-RECORD

In anticipation of the Director's scheduled appearance before the Senate Judiciary Committee this Thursday, May 20th, we are trying to confirm the number of times we have used Delayed Notice (so-called "Sneak and Peek") Warrants, FISA Roving Wiretaps, and FISA Orders for Tangible Things (i.e., so-called Section 215 Orders), since passage of the USA PATRIOT Act.

I realize there are several potential complications with compiling such numbers (e.g., Delayed Notice Warrants used in traditional criminal cases, classification issues re 215 Orders, etc.). Nevertheless, if any of you could provide some input on this, it would be very helpful. We can almost guarantee the Director will be asked about the numbers when he testifies.

Is DOJ compiling numbers? Is there anyone at OLP or OIPR who may know?

Thanks,

[redacted] b2
Office of Congressional Affairs b6
[redacted] b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OGC) (FBI)

From: [redacted] Div09) (FBI) b6 b7C

Sent: Tuesday, May 11, 2004 5:23 PM

To: [redacted] (Div09) (FBI)

Subject: Sunset Provisions

~~SECRET~~
RECORD 66F-HQ-C1364260

[redacted] Attached are the two documents I provided to OPA [redacted] The 1st document is the summary of the field survey that I'm currently putting together. I did leave in the classified portions for you. The 2nd document was a brief summary we provided to DOJ in March. b6 b7C

The consistent comment from the field was that the information sharing provisions (203 and 218) were the most important provisions in the Patriot Act. As you know, they have significantly altered the way we conduct business on a daily basis. This was a consistent point made in the field responses. They pointed to the joint task forces, better communications with other agencies, better working relationships across the board because they are no longer stifled by fear that they may inadvertantly share information incorrectly, better use of resources, etc.

While we know that 218 opened the door for more communications from the intell to the criminal side, does NSLB have any opinion on what effect the expiration of 218 would have on the FISC court opinion? Would this essentially then rebuild the wall?

If I can help, please feel free to contact me.

[redacted] b2 b6 b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
DECLASSIFICATION EXEMPTION 1
~~SECRET~~

USA Patriot Act
Sunset Provisions
Field Office Comments
April 2004

Section 201 & 202 - Expanded Title III predicates

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing). Due to the timing and statutory placement of these two additional predicate offenses, it is likely that these are now included in the sunset provision.[1]

Survey Results: The respondents to the field survey indicated that there was at least one Title III order where terrorism was identified as the predicate offense.

Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. The Homeland Security Act later authorized disclosure to foreign investigative or intelligence officials and to any federal, state, local, and foreign official when it reveals a threat of attack.

Note: The Congressional Research Services (CRS) report to Congress on the sunset provisions erroneously states that "termination of authority under subsection 203(b) may be a little consequence."[2] In fact, the termination of this provision would have absurd results.

[redacted] Essentially [redacted]

b5

Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. The Homeland Security Act also added foreign intelligence and investigative officials to the list of receiving officials. Due to the

[1]See CRS Report for Congress, "USA Patriot Act Sunset: Provisions That Expire on December 31, 2005," dated January 2, 2004., CRS Report RS 21704.

[2]CRS Report RS 21704 at 5.

b1 ,b2, b5, b7E

[redacted] (S)

b1 ,b2, b5, b7E

[redacted] (S)

[redacted] (S)

[redacted]

Section 207 - Extended Duration for Certain FISAs b1 b2, b5, b6, b7C, b7E

Section 207 extends the standard duration for several categories of FISA orders.

[awaiting input from NSLB [redacted] on this] b6 b7C

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail.

[redacted] b1 [S]

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury. The Homeland Security Act modified this provision as it relates to the content of communications, but not as it relates to the records held by a service provider. For this reason, the Congressional Research Service concludes that only those provisions relating to the voluntary disclosure of records is subject to the sunset provision.[3]

[3]See CRS Report, page CRS-8.

[was 2702 (c)(3) part of this provision? - allows for voluntary disclosure of records to protect their own property and rights.]

(S)

b1

[S]

b1

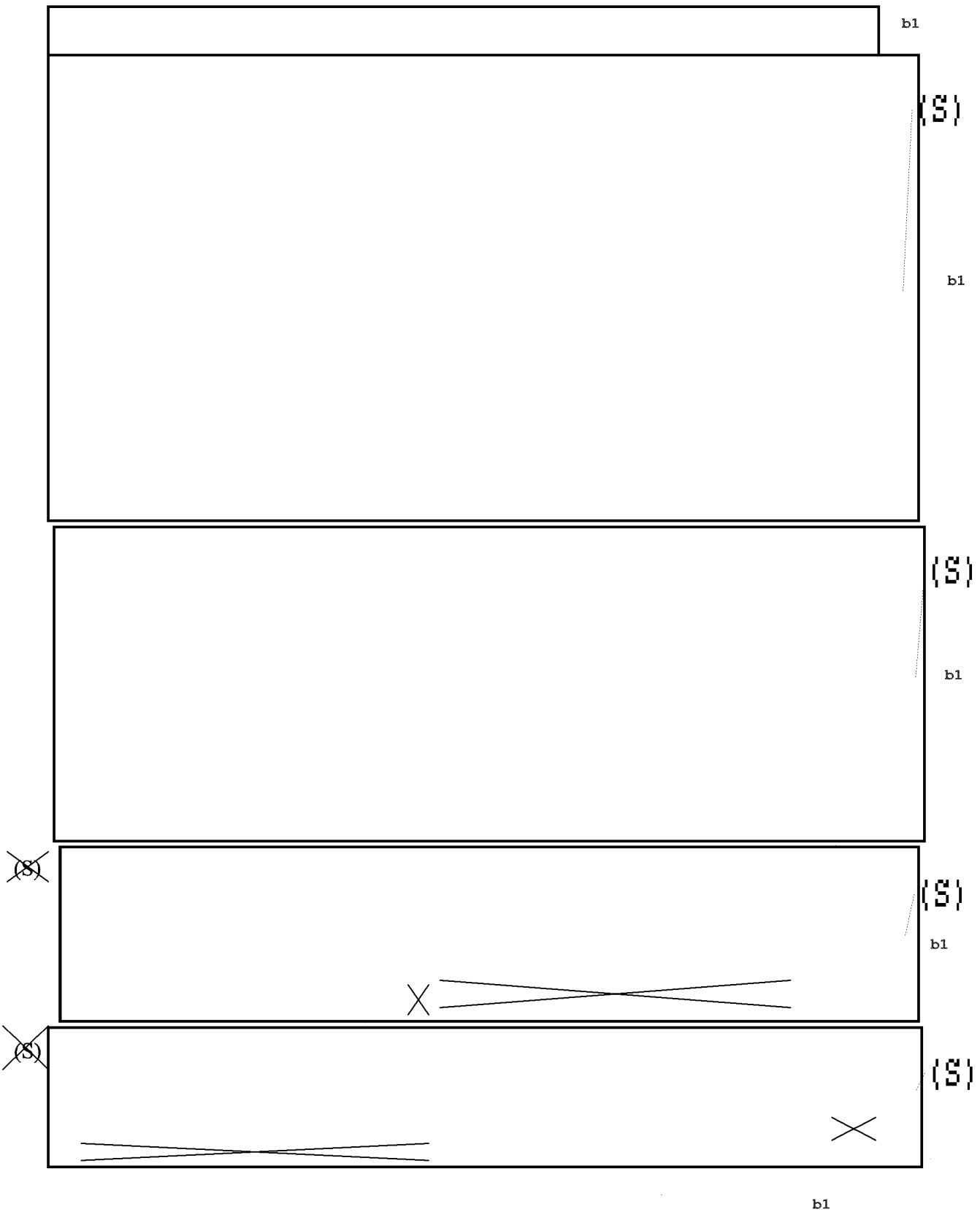
b7A

Section 214 - FISA Pen/Trap Authority

FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123

[S]

b1


b1
(S)
b1
(S)
b1
(S)
(S)
b1
(S)
b1

Section 215 - Access to Business Records under FISA

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records [redacted] to include "any tangible things (including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." b2 b7E

[redacted] [S]

b1

-Again the field offices consistently report their frustration with the length of time to get any approvals from OIPR to utilize these provisions.

One field office [redacted]) confused the 215 stating it was an NSL. Check with them to determine which it was. (These are different provisions).

b2

b7E

[redacted] (OGC) (FBI)

b6
b7C

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 04, 2004 4:54 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div09) (FBI)
Subject: Patriot Act Section 215 - after sunset

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

In compiling the information received from our recent field survey on the various sunset provisions, I'm also reading a report recently prepared by the Congressional Research Service for Congress on the various sunset provisions. The report states that if Section 215 is left to sunset, "the impact of expiration may be mitigated by changes in the law governing 'national security letters' that provide access to a wider range of business records"

This seems to be a confident statement that we will not be impacted by the expiration of Section 215. I know that I have already found an error in the report regarding Title III issues, and have alerted OEO to the misstatement so that it can be corrected. I bring this to your attention to provide you the same opportunity should you disagree with the statement.

If you have any questions, please feel free to contact me.

[redacted]

b2
b6
b7C

UNCLASSIFIED

[redacted] OGC) (FBI)

From: [redacted] (Div09) (FBI) b6
Sent: Wednesday, April 28, 2004 9:12 AM b7C
To: [redacted] (Div09) (FBI)
Subject: FW: 9/11 Commission Recommendations

UNCLASSIFIED
NON-RECORD

[redacted] Please see [redacted] email below and GC's input. Thanks.

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Wednesday, April 28, 2004 9:10 AM
To: [redacted] (Div09) (FBI) b6
Subject: FW: 9/11 Commission Recommendations b7C

UNCLASSIFIED
NON-RECORD

[redacted]

Below is the final that went through the GC. Spike provided input on this as well. Hopefully, you didn't spend too much time on this.

[redacted] b6 b7C

-----Original Message-----
From: Caproni, Valerie E. (Div09) (FBI)
Sent: Wednesday, April 28, 2004 8:26 AM
To: KELLEY, PATRICK W. (Div09) (FBI)
Cc: [redacted] (Div09) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: RE: 9/11 Commission Recommendations

UNCLASSIFIED
NON-RECORD

Those look good [redacted]

I have a question about the proposed change to AG exemptions: since it has to come to DC anyway (and presumably NSLU or ILU should be exercising some legal review of the requests) what is the real benefit of delegating down to the field offices? b5

Can we do something for Acting SACs? As I recall, OIPR takes the position that an Acting SAC is of a rank lower than deputy assistant director. Maybe limit it to ACting SACs that are SES?

-----Original Message-----
From: KELLEY, PATRICK W. (Div09) (FBI)
Sent: Tuesday, April 27, 2004 6:14 PM
To: Caproni, Valerie E. (Div09) (FBI)

Cc [redacted] (Div09) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] b6
(Div09) (FBI); [redacted] (Div09) (FBI) b7C
Subject: 9/11 Commission Recommendations

UNCLASSIFIED
NON-RECORD

Boss: here's the recommendations I'd like to send to [redacted] for consideration of the 9/11 commission. It's not clear what our deadline is bu[redacted] believes we need to get them ASAP. Thanks. b6 b7C

April 27, 2004

TO: [redacted] b6 b7C

FROM: Patrick Kelley, Deputy General Counsel

Subj: Recommendations to the 9/11 Commission

The following recommendations are forwarded for possible consideration by the 9/11 Commission. b5

[redacted]

b5

b5

b5

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Tuesday, April 27, 2004 10:26 AM
To: [redacted] (Div09) (FBI)
Cc: [redacted] Div09) (FBI)
Subject: RE: Ponies

b6
b7C


sample letter.wpd (31 KB)


2702-PA_letter v2.wpd (33 KB)

UNCLASSIFIED

NON-RECORD

[redacted] b6 b7C

The first letter looks very well done. It clearly explains that this is a voluntary disclosure by the ISP, an important point. I offer the following comments:

1 - The standard for voluntary disclosure under 2702(b)(7) changed slightly with the Homeland Security Act. It now states that the provider must believe in "good faith" that the emergency exists. This was due to pressure from the ISPs. They didn't want to be in the position to have to determine if the law enforcement request was reasonable (under the old "Patriot Act" standard), but instead only to be held responsible to act in good faith. Also, the Homeland Security Act eliminated the requirement that the emergency be in regard to "immediate" death or serious physical injury, but instead that immediate action be required. (for a more detailed explanation, see the EC we drafted on this - that (FYI) is still not signed). (I edited the letter in this regard and attached it for your review)

Note - however, that these changes to the standard only effected (b)(7) regarding disclosure of content, and did not change the old standard for (c)(4) regarding records. Thus, the way this letter spells out the standard for both content and records is good. b5

[redacted] (see EC 66F-HQ-1085159-56 dated 10/14/03)

[redacted] b5

[redacted] b5

[redacted]

b5

Again, this letter is very well done. These comments are intended to be only minor. It does provide more details than I have seen in the past, however, the past does not always dictate what is best. I have attached 2 documents. First, my minor edits to the statutory language in the letter, and second, the sample letter I attached to the EC I drafted.

Finally, [redacted] you may not be aware that the reporting requirement for these disclosures under the Homeland Security Act has expired. We are no longer reporting these disclosures to DOJ as we did througout last year. However, because it is a sunset provision, we are trying to keep records on this use of this provision in order to justify the need and provide solid examples of its use. b6 b7C

If there is anything further I can do to assist, please don't hesistate to contact me.

Best wishes -

[redacted]

-----Original Message-----
From: [redacted] (Div09) (FBI) b6 b7C
Sent: Monday, April 26, 2004 9:54 AM
To: [redacted] (Div09) (FBI)
Subject: FW: Ponies

UNCLASSIFIED
NON-RECORD

[redacted] Could you review the first letter and let me know if it conforms with other letters the FBI has used. Thanks. [redacted] b6 b7C

-----Original Message-----
From: [redacted] (WF) (FBI)
Sent: Monday, April 26, 2004 9:38 AM b6
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI) b7C
Cc: Curran, John F. (Div09) (OGA)
Subject: FW: Ponies

UNCLASSIFIED
NON-RECORD

Attached is a sample of the waranntless "Patirot Act" letters that ITOS is providing as a "go by".

-----Original Message-----
From: [redacted] (WF) (FBI) b6
Sent: Monday, April 26, 2004 8:46 AM b7C
To: [redacted] (WF) (FBI)
Subject: Ponies

UNCLASSIFIED
NON-RECORD

b6
[redacted] b7C

I've attached a couple of ponies regarding ISPs that I got from some recent training. They are "Patriot Act" letters that look interesting. Below are comments that came with them from one of the CXS guys at HQ.. [redacted]

I've attached an Emergency Request that was done stright out of ITOS II here -the SC signed off on it and I do not think ITOS II is routing them by NSLB

(but they should atleast report them, after the fact). The office will have to track and report how many of these are done, so check with your CDC for a control file number to route them to. I know SAC's can sign them in the field, but I do not think they can delegate that authoirty down (the same as NSL'S).

Oh, and the statute is 2703 on the criminal requests, 2703d for the logs, and 2703f for the preservation request.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

b6
b7C

[redacted] (OGC) (FBI)

From: [redacted] (WF) (FBI)
Sent: Monday, April 26, 2004 9:38 AM
To: [redacted] (Div09) (FBI) [redacted] (Div09) (FBI)
Cc: Curran, John F. (Div09) (OGA)
Subject: FW: Ponies

2702-PA_letter.wp (29 KB) PArequest.wpd (28 KB)

UNCLASSIFIED
NON-RECORD

Attached is a sample of the waranntless "Patirot Act" letters that ITOS is providing as a "go by".

-----Original Message-----
From: [redacted] (WF) (FBI)
Sent: Monday, April 26, 2004 8:46 AM
To: [redacted] (WF) (FBI)
Subject: Ponies

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

I've attached a couple of ponies regarding ISPs that I got from some recent training. They are "Patriot Act" letters that look interesting. Below are comments that came with them from one of the CXS guys at HQ.. [redacted]

I've attached an Emergency Request that was done stright out of ITOS II here -the SC signed off on it and I do not think ITOS II is routing them by NSLB (but they should atleast report them, after the fact). The office will have to track and report how many of these are done, so check with your CDC for a control file number to route them to. I know SAC's can sign them in the field, but I do not think they can delegate that authoirty down (the same as NSL'S).

Oh, and the statute is 2703 on the criminal requests, 2703d for the logs, and 2703f for the preservation request.

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI)

b6
b7C

From: Caproni, Valerie E. (Div09) (FBI)
Sent: Wednesday, April 21, 2004 8:24 AM
To: BOWMAN, MARION E. (Div09) (FBI); [redacted](Div09) (FBI)[redacted] (Div09) (FBI); Curran, John F. (Div09) (OGA)[redacted]Div09) (FBI)[redacted] (Div09) (FBI[redacted]
Subject: RE: Patriot Act

UNCLASSIFIED
NON-RECORD

This has not yet been fully cleared for release by DOJ so do not disseminate outside of NSLU. Also, if there is anything in it that gives anyone concern (i.e., are they disclosing too much about sources and methods) please let me know ASAP.

-----Original Message-----
From: BOWMAN, MARION E. (Div09) (FBI)
Sent: Wednesday, April 21, 2004 8:18 AM
To: [redacted](Div09) (FBI)[redacted](Div09) (FBI); Caproni, Valerie E. (Div09) (FBI); Curran, John F. (Div09) (OGA)[redacted]Div09) (FBI)[redacted](Div09) (FBI)[redacted]
Subject: Patriot Act

b6
b7C

UNCLASSIFIED
NON-RECORD

The attached was prepared by DOJ for the campaign to save the Patriot Act provisions that are slated to expire.

UNCLASSIFIED

UNCLASSIFIED

[redacted] (OGC) (FBI)

b6
b7C

From: BOWMAN, MARION E. (Div09) (FBI)
Sent: Wednesday, April 21, 2004 8:18 AM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); Caproni, Valerie E. (Div09) (FBI); Curran, John F. (Div09) (OGA); [redacted] Div09) (FBI); [redacted] Div09) (FBI); [redacted]
Subject: Patriot Act

UNCLASSIFIED
NON-RECORD

The attached was prepared by DOJ for the campaign to save the Patriot Act provisions that are slated to expire.

UNCLASSIFIED

[redacted] (OGC) (FBI)

b6

From: [redacted] (Div09) (FBI) b7C

Sent: Monday, April 19, 2004 9:17 AM

To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)

Subject: RE: Restrictions on sharing information with TTIC

UNCLASSIFIED
NON-RECORD

Has there been any further evauation of this position?. I haven't seen any replies to this email.

-----Original Message-----
From [redacted] (Div09) (FBI)
Sent: Thursday, March 04, 2004 3:19 PM
To: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: Restrictions on sharing information with TTIC

b6
b7C

UNCLASSIFIED
NON-RECORD

Section 203(d) of the Patriot Act provides that "Notwithstanding any other provision of law" it is lawful to share foreign intelligence or counterintelligence (as defined in 50 USC 401a) or foreign intelligence information obtained as part of a criminal investigation with any federal law enforcement, intelligence, protective immigration, national defense, or national security official in order to assist the receiving official in his official duties. The receiving official may use the information only as necessary in the conduct of his official duties subject to any limitation on the unauthorized disclosure of such information.

[redacted] b5

[redacted] b5

UNCLASSIFIED

UNCLASSIFIED

[redacted](OGC) (FBI)

From: [redacted](Div09) (FBI) b6 b7C
Sent: Tuesday, March 30, 2004 3:42 PM
To: [redacted]Div00) (FBI)
Cc: Curran, John F. (Div09) (OGA); BOWMAN, MARION E. (Div09) (FBI) [redacted] (Div09) (FBI); KELLEY, PATRICK W. (Div09) (FBI)
Subject: RE: DOJ Request for Response, due to DOJ MARCH 31

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-06-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

UNCLASSIFIED
NON-RECORD

[redacted] Here are your responses. b6 b7C

Question: Has the FBI served any NSLs on libraries since September 11, 2001 - yes or no - and if yes, on how many occasions?

Answer: No.

Question: Since September 11, 2001, what guidance has the Department provided to the FBI about the use of NSLs to obtain records from libraries and/or bookstores?

Answer: To the best of our knowledge [redacted] b5

-----Original Message-----
From: [redacted](Div00) (FBI)
Sent: Monday, March 29, 2004 8:21 AM b6
To: [redacted](Div09) (FBI) b7C
Subject: RE: DOJ Request for Response, due to DOJ MARCH 31

UNCLASSIFIED
NON-RECORD

[redacted] b5

[redacted] b6 b7C

[redacted]email made it sound as though you would collect more info than that, and I'd love for you to avoid additional work, if possible.

Thanks. Sorry you keep inheriting these.

[redacted]
Office of Congressional Affairs b2
JEH Building Room 7252 b6
[redacted] b7C

-----Original Message-----
From: [redacted]Div09) (FBI)
Sent: Sunday, March 28, 2004 10:36 AM
To: [redacted](Div00) (FBI)
Cc: Curran, John F. (Div09) (OGA); KELLEY, PATRICK W. (Div09) (FBI) [redacted] (Div09) (FBI); [redacted](Div09) (FBI)

Subject: RE: DOJ Request for Response, due to DOJ MARCH 31

UNCLASSIFIED
NON-RECORD

I'll be out of the office this week. Per this e-mail I have forwarded your request to who will be b6 b7C

- Could you please assist with these questions? I am not aware of any guidance issued by DOJ re:use of NSLs. Maybe may know. Also, do we keep track of what entity we served NSLs on The statistics we send to DOJ do not break it down this way. We may have to review all the ECs we have received to determine who was served with an NSL. b5 b6 b7C

-----Original Message-----
From: (Div00) (FBI)
Sent: Friday, March 26, 2004 5:14 PM
To: (Div09) (FBI) b6
Cc: Curran, John F. (Div09) (OGA); KELLEY, PATRICK W. (Div09) (FBI) b7C
Subject: DOJ Request for Response, due to DOJ MARCH 31
Importance: High

UNCLASSIFIED
NON-RECORD

DOJ has just asked us to very quickly prepare responses to the following questions. The bad news is that their deadline is March 31 because of an upcoming hearing. The good news is that the questions are fairly narrow.

Could you please respond to the following? If I need to seek assistance from someone else, please let me know. Obviously, time is limited. I'm happy to come and pick up any documents responsive to 6A (note that they have not asked for FBI guidance, but only DOJ guidance to the FBI).

b5

Thanks for your help.

b5

[redacted] b5

[redacted] b5

[redacted]
Office of Congressional Affairs b2
JEH Building Room 7252 b6
[redacted] b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

b6
b7C

[redacted] OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Monday, March 08, 2004 2:33 PM
To: BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI) [redacted]
E; Curran, John F. (Div09) (OGA)
Subject: FW: PATRIOT ACT SUNSET PROVISIONS

Sensitivity: Private

DECLASSIFIED BY 65179 DMH/CLS
ON 09-07-2005

CA# 05-CV-0845

UNCLASSIFIED
NON-RECORD

FYI

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Monday, March 08, 2004 1:16 PM
To: [redacted] (Div09) (FBI)
Cc: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (RH); MANN, PHILIP J. (NF) (FBI); [redacted] (Div09) (FBI); [redacted]
Subject: RE: PATRIOT ACT SUNSET PROVISIONS
Sensitivity: Private

[redacted]

b5
b6
b7C

SSA [redacted]
[redacted] Office of Division Counsel [redacted]

b2
b6
b7C

Privileged and ~~Confidential~~

>>> [redacted] (Div09) (FBI) 03/04 3:17 PM >>>
UNCLASSIFIED
NON-RECORD

See the attached EC that was uploaded today. See 66F-HQ-1364260-5.

UNCLASSIFIED

[redacted] OGC) (FBI) b6 b7C

From: Caproni, Valerie E. (Div09) (FBI)

Sent: Thursday, March 04, 2004 3:33 PM

To: [redacted] (Div09) (FBI); WAINSTEIN, KENNETH L ; BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); Curran, John F. (Div09) (OGA); MUELLER, ROBERT S. III

Subject: Section 215 of the Patriot Act

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

SENSITIVE BUT UNCLASSIFIED

b5

[redacted] (OGC) (FBI)

From: [redacted]
Sent: Friday, February 13, 2004 5:48 PM
To: BOWMAN, MARION E.; [redacted]
Cc:
Subject: RE: Pending Issue Papers

b6
b7C

director issue paper.wpd (8 KB... civliberty issues.wpd (15 KB)

Attached are two papers I did on impact of post 9/11 FBI investigations and Patriot Act on civil liberties and effect on mosques and libraries for the general counsel that may be suitable to go into issue papers. I also have some stuff on use of other PA provisions on FBI investigations and am seeking some more--when I get that I'll put it together and send it to you.

[redacted]

b6
b7C

-----Original Message-----
From: BOWMAN, MARION E.
Sent: Wednesday, February 11, 2004 1:44 PM
To: [redacted]
Subject: FW: Pending Issue Papers

b6
b7C

Can your three put your heads together on this?

-----Original Message-----
From: [redacted]
Sent: Wednesday, February 11, 2004 1:56 PM
To: [redacted] BOWMAN, MARION E.
Subject: Pending Issue Papers

b6
b7C

Gentlemen,

Sorry to ask this of you, CTD needs some help putting together "Issue Papers" for the Director's upcoming testimony before the Senate & House Appropriation Committees regarding the FY2005 budget.

The hearings are open to the public, and therefore unclassified. Two of the topics we need help with deal with issues that NSLB has an intimate knowledge of. The first being FISAs, which we need an overview of the improvement made in the past year, what legal limitations we face, and any issues we may have with training as it relates to FISAs.

The second topic that needs to be addressed is the PATRIOT ACT, as it relates to:

1. How it has helped the FBI/Use of Expanded Authorities
2. Civil Liberties
3. Libraries
4. Mosques

I have been tasked to find this information and put it together for the front office by next Wednesday, 02/18/2004. Would someone from your Division be able to assist on these two issues? I want to make sure it is right with NSLB.

Thank You,

SSA [redacted] b2
CTD-Executive Staff b6
[redacted] b7C

Impact of the Patriot Act on Libraries/Bookstores and Mosques

Libraries/Bookstores: Despite media reports to the contrary, nothing in the Patriot Act is directed at or even mentions libraries or bookstores. Section 215 does permit the FISA Court to issue an order to produce "tangible things," including business and other records, in support of a foreign intelligence or international terrorism investigation. It also prohibits notice to the customer whose records are ordered produced.

This section has not yet been used at all and therefore there has been no actual impact on libraries or bookstores. [redacted] This authority cannot and will not be used to monitor the reading habits of library patrons or even those of certain groups or members of certain organizations. If used, it would be used in a specific case for a specific individual and based on a valid investigative reason. For example, [redacted] b5

Therefore, if Section 215 were ever used to obtain patron records from a library or bookstore, its impact would be case specific, fleeting, isolated and, in the end, inconsequential to the day-to-day business of the Nation's libraries and bookstores.

[redacted] b5

[redacted] b5

*** Issue: Whether the FBI is using its new powers under the AG Guidelines to monitor the activities of lawful demonstrators/protestors under the guise of fighting terrorism.**

b5

*** Issue: Whether Section 215 of the Patriot Act permits the FBI to subvert due process by collecting information about Americans without notice or the opportunity to challenge the collection in a court of law.**

Comment: *Section 215 of the Patriot Act permits the FISA court to issue an order to a third party owner/custodian of records pertaining to a party to produce those records in support of a national security investigation and, in addition, to prohibit notice to the party. This section (which has not been used to date) not only contains built-in judicial and congressional (requires reporting to Congress) oversight, it may only be used in support of a duly authorized and open national security investigation and must be viewed in the context of the other federal laws that regulate the collection of information. The Privacy Act is still alive and well and prohibits the collection and retention of personal information except for valid law enforcement purposes. Moreover, basic due process still requires that, before any such information can be used to the detriment of any person, that person will have his or her day in court to contest the information and the manner by which it was collected. The Patriot Act did nothing to change this basic tenet of American law. Finally, the no-notice provision, in addition to being essential to the FISA process, is, in practice, not much different than the use of federal grand jury subpoenas. Although the recipients of these subpoenas may resist compliance and gain access to court to state his case, the party to whom the records pertain has no such right, has no right to be notified that his/her records are sought, and a court may in fact prohibit notice to the party. Many such subpoenas are issued in the case of parties who are never indicted and therefore never know that their records were seized.*

*** Issue: Whether Section 213 of the Patriot Act violates the constitutional rights of citizens by authorizing a judge to delay the required notice of the execution of a Rule 41 search warrant for a reasonable time.**

Comment: *This section is merely a codification of the delayed notice or "sneak and peak" warrant already approved by the federal judicial system. The courts have found that*

notice of the execution of a search warrant is not a constitutional requirement and have found that a reasonable delay of notice does not undermine Rule 41's requirement that notice be provided. All Section 213 did was codify existing law. In addition, it made it clear that delay must be for good cause, as must any extension of delay originally granted, and, finally, that any such warrant may not authorize the seizure of any property. The longest delay known to us at OGC has been 90 days but, again, the judge must be satisfied that delay and its particular length are justified by the reasons offered by the agent. In the end, all of this process will be exposed and the defendant will have the opportunity to contest the delay and seek a remedy.

*** Issue: Whether the FBI is collecting criminal evidence for prosecution using the national security intelligence collection processes of the Patriot Act with their lower standards and the absence of a criminal predicate. This is one of the fundamental criticisms of both the Patriot Act and the other post 9/11 regulations, directives, and guidelines. In summary, it is that because the "wall" between criminal prosecutions and national security investigations has been torn down, it will be easier for the government to collect information using national security legal process (NSLs, FISAs, foreign intelligence methods) which do not require a criminal predicate and turn that information into criminal evidence for prosecution--evidence that could not have been obtained through criminal process and which before the Act could not have been used to prosecute.**

Comment: *One answer to this is that, in fact, under the FISA statute, information obtained through the FISA process and other means always could have been used to prosecute and, in many instances, has. Espionage prosecutions, for example, have seen this. The Patriot Act and ensuing guidelines just makes it easier. Another answer to this is that, although the wall has come down and information sharing between the IC and prosecutors is easier, the burden of the prosecutor to prove his case through admissible, reliable, and properly authenticated evidence has not changed. In addition, the rights of the defendant to contest the evidence and the manner by which it was obtained was not affected by the Patriot Act. A third answer is that, although no criminal predicate is required, each of these national security processes has threshold criteria--such as probable cause for a FISA warrant--that are comparable to those in a corresponding criminal process. A Section 215 order compares roughly to a FGJ subpoena (plus judicial approval); an NSL for subscriber records to a FGJ or admin subpoena; a delayed-notice search warrant to a FISA physical search order.*

*** Issue: Whether the FBI's comprehensive data bases of known or suspected terrorists includes ordinary citizens and resident aliens whose names and identities are included by mistake and who have no recourse when they are denied travel and other basic rights.**

Comment: *The data bases that are, and will be, established pursuant to the Patriot Act's requirement to track foreign terrorists and the President's creation of the Terrorist Threat Integration Center (and the Terrorist Screening Center) have many contributors--not just the FBI. For the FBI's part, internal policy will restrict the input of personal data to known or suspected terrorists who are the subjects of duly authorized FBI national security investigations. In other words, the same criteria and predication in the Attorney General Guidelines that*

[redacted] OGC) (FBI)

From: [redacted]
Sent: Wednesday, February 11, 2004 4:50 PM
To: Caproni, Valerie E.
Cc: [redacted]
Subject: Sunset provisions

b6
b7C

[redacted] had a good thought about how to get what OLP wants to prepare for the "sunset." Attached is a draft of an EC that we sent out in June 2002 about the Patriot Act to all Fos. In it, we say that several provisions would sunset unless renewed and for that reason offices were "encouraged" to keep records of their use of these provisions. In addition, CDCs were advised to do that at the CDC Conference and given a handout of what provisions would sunset and again asked them to keep examples of their usefulness and to send them to ILU. We haven't received any.

We should do an EC from a senior HQ official (you'll do or the DD) reminding the Fos of this earlier advice and then tasking them (SACs/ADICs) to collect stats/examples or at least to summarize in a narrative the value of each provision and why it should stay alive. I can write that if you want.

In addition, DOJ (OEO) should have stats on the 203/905 dissemination of FGJ and T-3 info to the IC and we could refer OLP to them. Also, we do have some stats about § 212 (voluntary emergency disclosure of e-mail content by an ISP) in my office. Perhaps, as well, OLP could be directed to OIPR for some of the FISA sunset provisions--214 (pen/trap trace), 206 (roving FISAs).

[redacted]

[redacted]

b6
b7C

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6 b7C
Sent: Thursday, March 17, 2005 2:37 PM
To: [redacted] OGC) (FBI); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); [redacted] OGC) (FBI) [redacted] OGC) (FBI) [redacted] (OGC) (FBI); [redacted] OGC) (FBI)
Subject: RE: Patriot act provision re: public libraries

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH/CLS
CA# 05-CV-0845

UNCLASSIFIED
NON-RECORD

[S]

[redacted] Since the passage of the Patriot Act, we know that there was one NSL [redacted] for certain records. I can dig up the example if you need it. There have been no business records served on libraries (or bookstores for that matter). [redacted] b1 b5 b6 b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 17, 2005 1:00 PM
To: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: RE: Patriot act provision re: public libraries b6 b7C

UNCLASSIFIED
NON-RECORD

I mean business records request (Section 215). Right [redacted] b6 b7C

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Thursday, March 17, 2005 12:55 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] OGC) (FBI) [redacted] OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: Patriot act provision re: public libraries

UNCLASSIFIED
NON-RECORD

CTD is assisting Office of Congressional Affairs prepare the Director for testimony re: patriot act and its sunset provision (December, 2005?). You are probably going to be getting questions about success stories related to the changes made by the Act. One question I have gotten is about the provision permitting the FBI to review records at a public library. CTD is having difficulty determining if this was ever utilized. Does anyone know?

I haven't even been able to determine what the procedure would have been for anyone seeking to use this provision, does anyone know what the process would be?

DATE: 12-30-2005
CLASSIFIED BY 65179DMH/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-30-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[redacted]
NSLB - CTLU 1
LX 1 room 5S 217
Outside #: [redacted]
Internal #: [redacted]
Pager: [redacted]

b2
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

[redacted] (OGC) (FBI)

From: [redacted] (OGC)(FBI) b6 b7C
Sent: Thursday, March 17, 2005 1:01 PM
To: [redacted] (CTD) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: Follow-up Re Director's Senate Testimony

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C
[redacted]

Here's some additional guidance beyond that which OCA offered (below).

Some examples of PATRIOT Act success that may prove helpful:

- **Sharing grand jury, Title III, and criminal investigative information.** [Sec. 203 was intended to eliminate barriers to timely sharing of information between criminal investigators and other entities (e.g., the IC, ICE, DoD, etc.) involved in the protection of national security. It gave the FBI full discretion to share criminal investigative information, regardless of its source, whenever it involves foreign intelligence information.] b1 ,b2, b7E

- **"Roving" FISA ELSUR authority.** [Sec. 206 was intended to counter a FISA target's attempts to use tradecraft to defeat ELSUR [redacted] avoiding the [redacted] [S]

- **Changes in FISA PR/TT authority.** [Sec. 214 eliminated one of the showings that was previously required--i.e. [redacted] Now, the focus is simply on relevance to an investigation.] b2 b7E

- **Changes in FISA business records authority.** [Sec. 215 assists the FBI in compelling production of business records. Previously, the FBI encountered situations in which holders of relevant records refused to produce them absent a subpoena or other compelling authority. Now, the FBI can seek a FISA court order for any such materials. Furthermore, the categories of things now attainable are much broader [redacted]

- Also, if your folks happen upon any instances in which **library records** were obtained, that information would likewise be helpful. b2 b7E

Again, sincere thanks to you and your folks for all your help.

[redacted]OGC) (FBI)

b6

From: [redacted]OGC) (FBI) b7C

Sent: Monday, March 21, 2005 2:13 PM

To: [redacted]OGC) (FBI); [redacted]OGC) (FBI)

Subject: Revised PATRIOT Act Director Testimony

Importance: High

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

UNCLASSIFIED
NON-RECORD

See attached.

UNCLASSIFIED

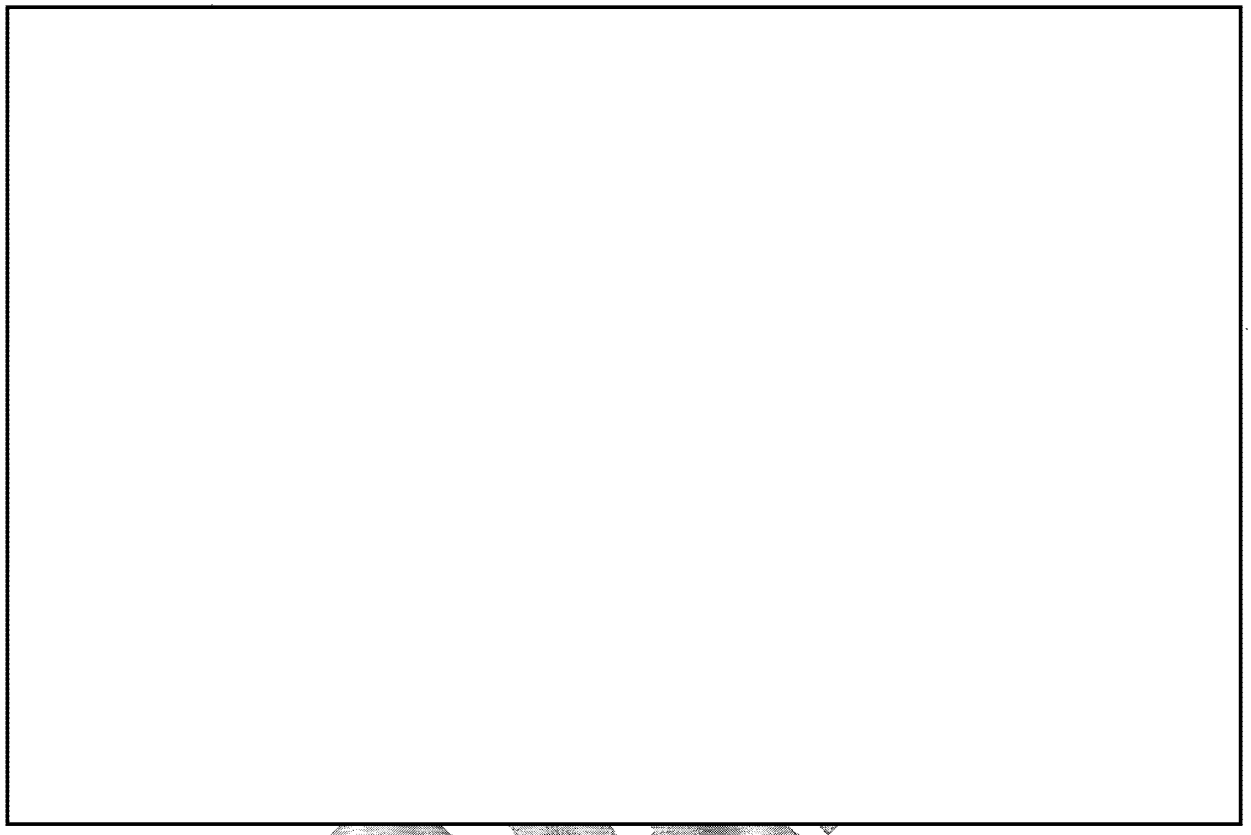
REVISED 3/21/05

FBI
Office of General Counsel
National Security Law Branch

March 21, 2005

The Office of General Counsel has prepared this draft testimony at the request of the Office of Congressional Affairs. This request was received by the author of the draft on March 16, 2005 and the author was required to complete this draft on March 21, 2005. The Office of General Counsel does not have access to the full library of testimony given on this subject and must rely on the Office of Congressional Affairs to ensure that all testimony is consistent with prior testimony given by the Director and other senior FBI officials. The Office of General Counsel has requested that the Counterterrorism Division's International Terrorism Operations Sections I & II provide specific examples for use in this testimony. Such examples have not yet been received by the Office of General Counsel. The author of this draft testimony has therefore relied upon the examples from prior FBI testimony and DOJ reports to Congress.

b5



ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the PATRIOT Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address two areas in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

b5

Administrative Subpoenas

[redacted]

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and currently there is no enforcement mechanism. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously this may not be the most effective process to undertake. Furthermore, FISA disclosure rules would apply, affecting the FBI's ability to share information expeditiously. The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal could provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the PATRIOT Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, by granting further modifications to the Foreign Intelligence Surveillance Act and by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today.

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Wednesday, March 23, 2005 9:27 AM b7C
To: Caproni, Valerie E. (OGC) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: Updated Draft Director's Senate Judiciary Testimony on PATRIOT ACT

UNCLASSIFIED
NON-RECORD

Valerie:

[redacted] asked me to make a few more tweaks and then to e-mail the attached to you.

Thanks, b6 b7C

[redacted]

==========

[redacted]
Assistant General Counsel
National Security Law Branch
FBIHQ Room 7975
Direct Line: [redacted]
Unclassified Fax: [redacted]
Secure Fax: [redacted]

b2 b6 b7C

UNCLASSIFIED

[redacted] (OGC) (FBI) b6 b7C

From: [redacted] (OGC) (FBI)
Sent: Wednesday, March 30, 2005 8:05 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (OGC)(FBI); THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Roving Authority

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Please note:

The number of Section 206 orders since the Patriot Act's signing to date [redacted] [S] b1

[redacted]
National Security Law Policy and Training Unit
FBI HQ Room 7975
STU III: [redacted]
Unclassified Fax: (202) 324-1023 b2
Secure Fax: (202) 324-9361 b6
-----Original Message----- b7C
From: [redacted] (OGC) (FBI)
Sent: Monday, March 28, 2005 4:36 PM
To: [redacted] (OGC) (OGA)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Roving Authority

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Perfect. Thanks.

-----Original Message----- b6
From: [redacted] (OGC) (OGA) b7C
Sent: Monday, March 28, 2005 4:03 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: RE: Roving Authority

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted] just answered a similar question via an email from Valerie. The number of Section 206 orders since the Patriot Act's signing to date is [redacted] Does that give you what you need? Let me know if not [redacted]
[S] b1

-----Original Message----- b6
From: [redacted] (OGC) (FBI) b7C

Sent: Monday, March 28, 2005 10:10 AM
To: [redacted] (OGC) (OGA)
Cc: [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: Roving Authority

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

I am writing to follow up on a phone conversation I had with [redacted] last week before she left for vacation. Valerie Caproni has asked NSLB to determine how many times FISA Roving authority has been granted since the change in the law. [redacted] told me that you were compiling that information and other, similar, statistics. When you get the number, could please send it to us?

Thanks for your help.

b6
b7C

Best,

[redacted]

==========

[redacted]
Assistant General Counsel
National Security Law Branch
FBIHQ Room 7975
Direct Line: [redacted]
Unclassified Fax: 202.324.1023
Secure Fax: 202.324.9361

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

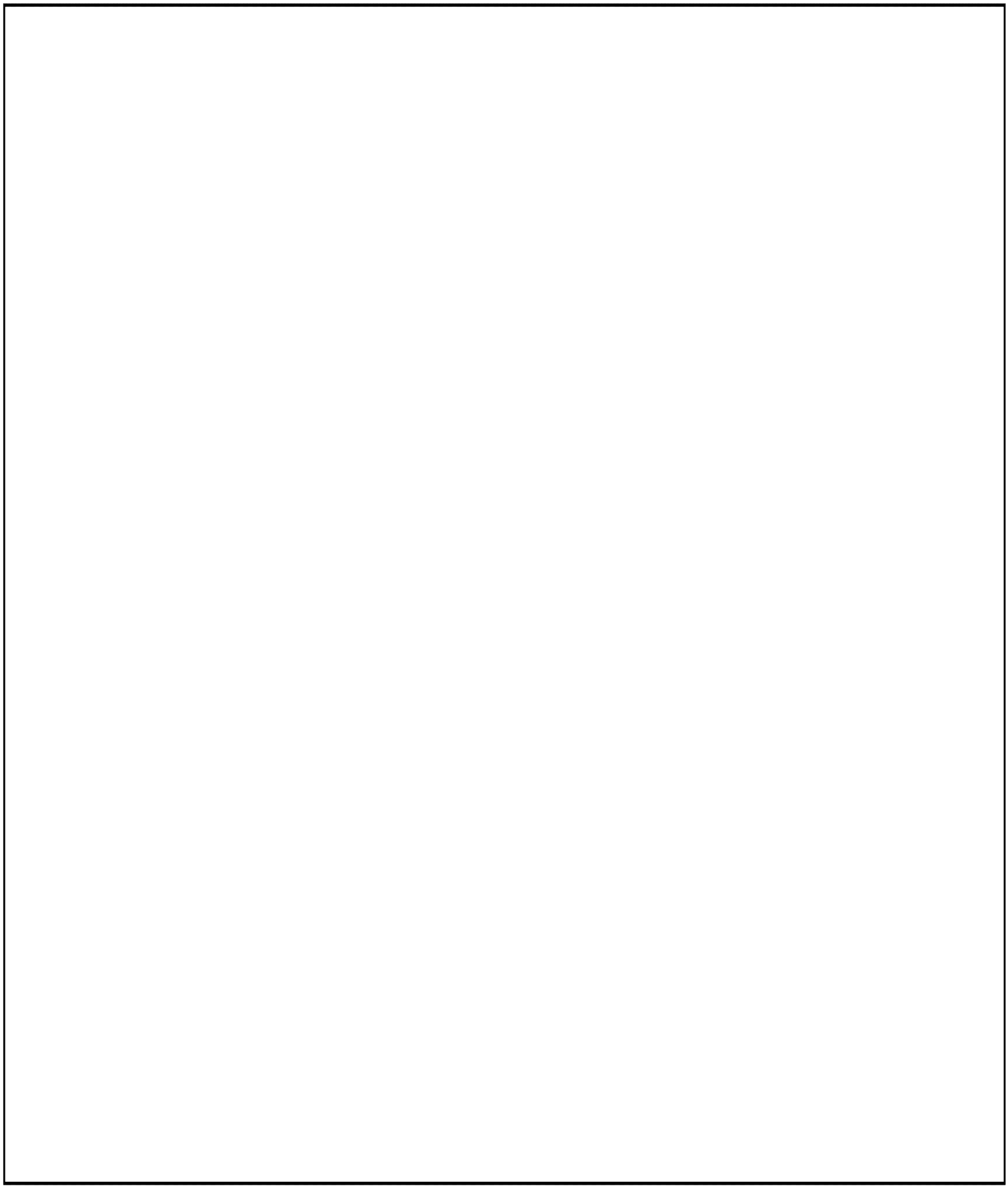
SENSITIVE BUT UNCLASSIFIED

DATE: 09-01-2005
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (C)
DECLASSIFY ON: 09-01-2030

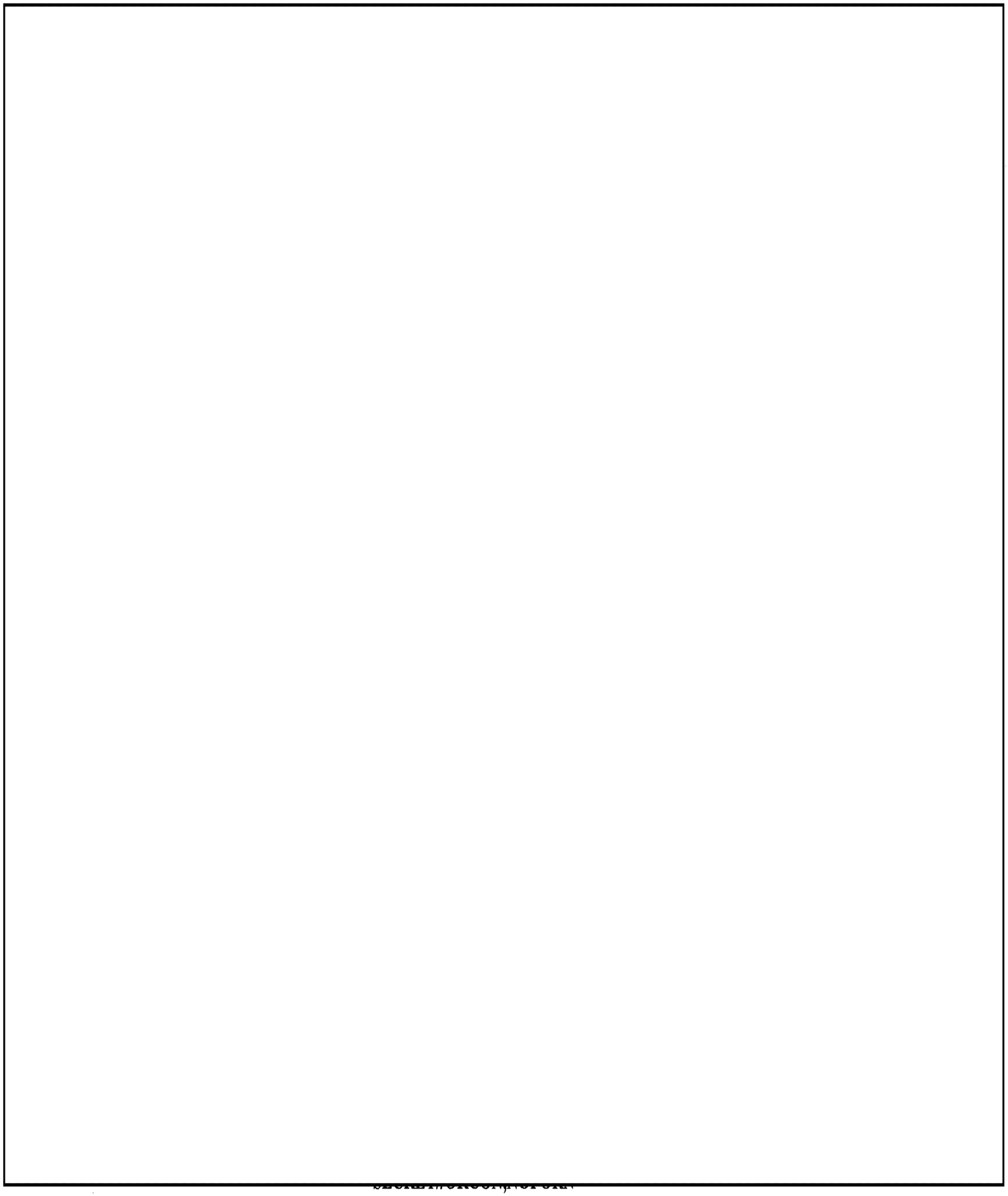
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1 ,b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E



b1 ,b2, b6, b7C, b7E



b1 ,b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E

b1 b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E

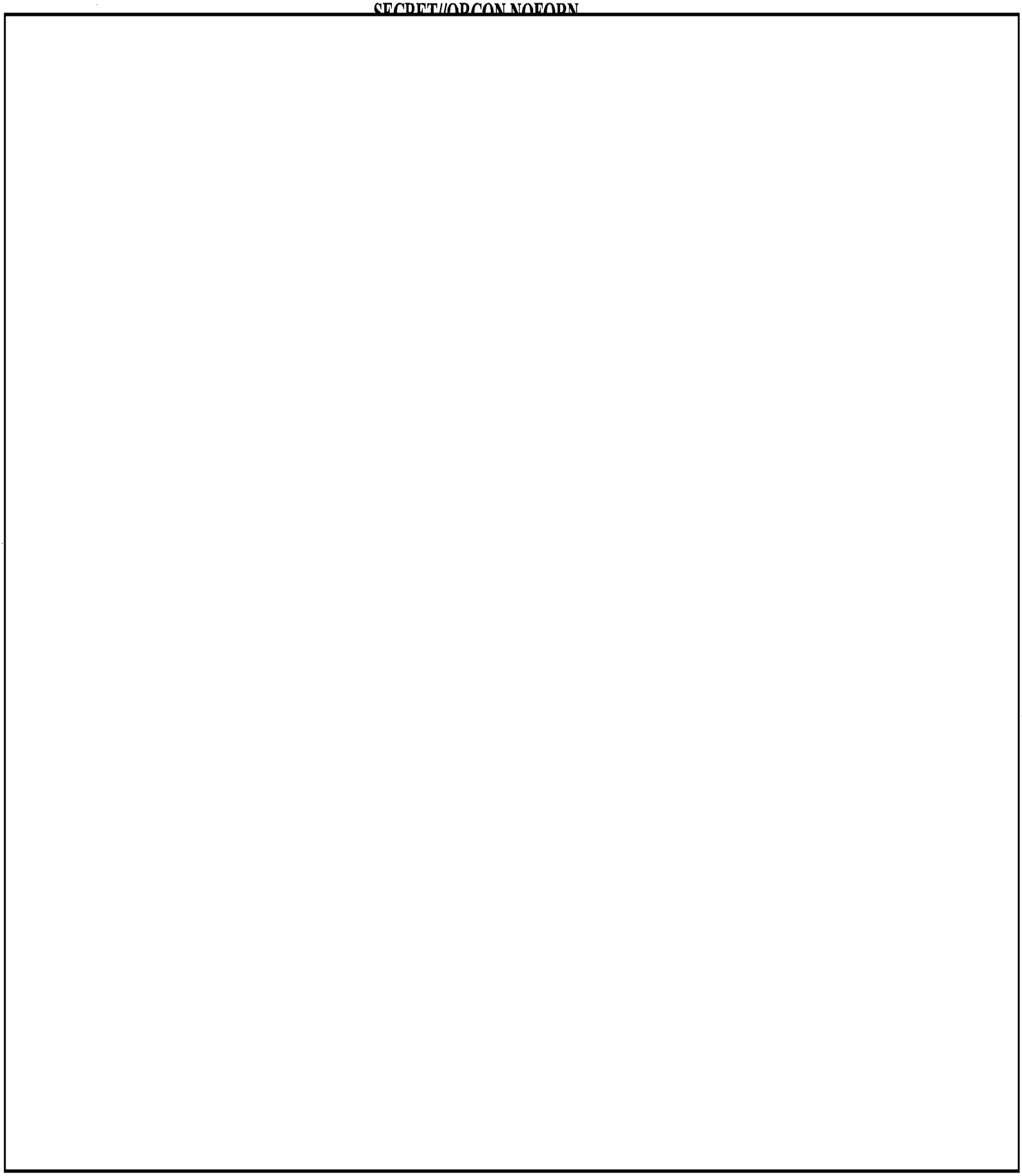
b1 ,b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E

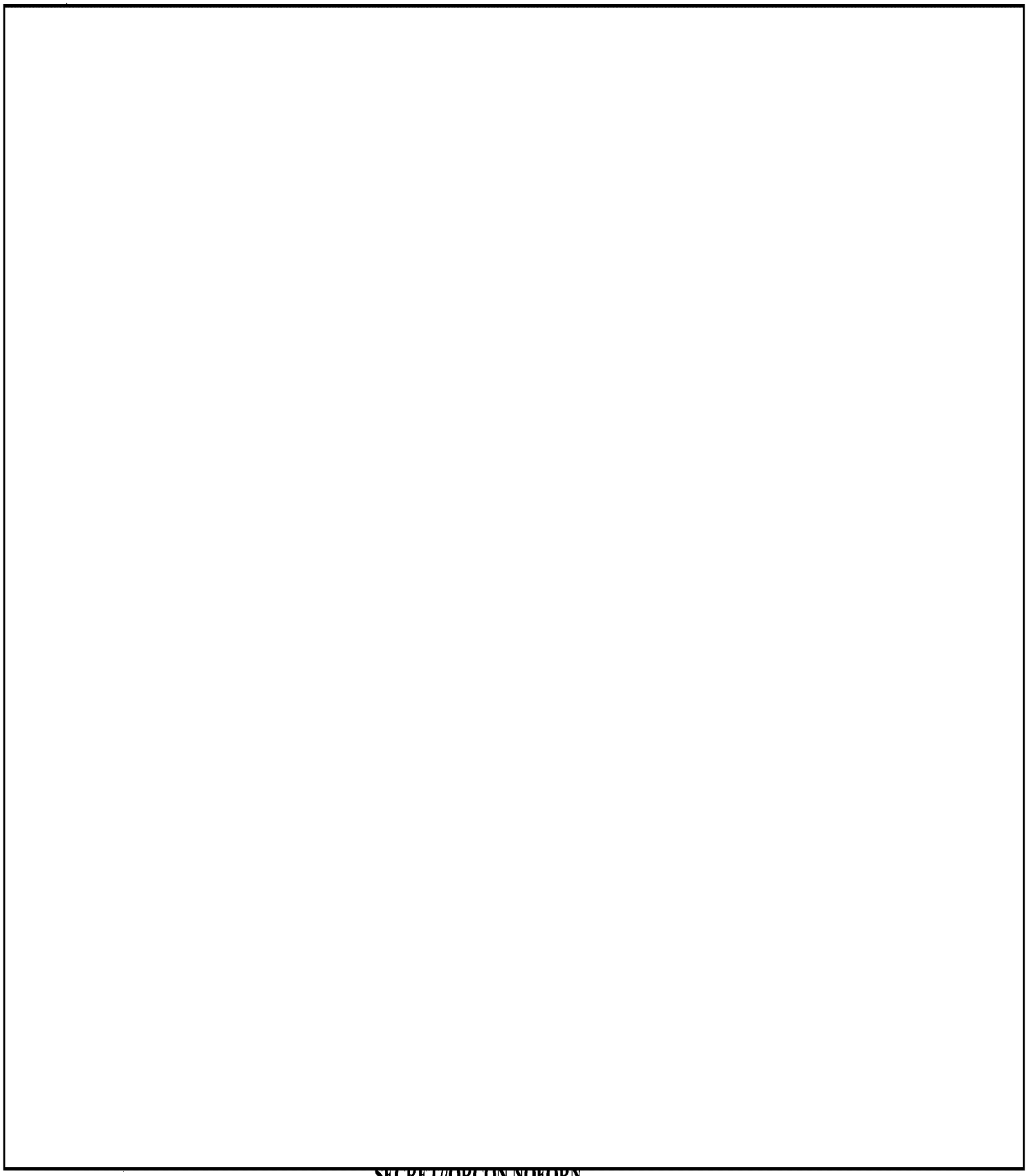
b1 ,b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E

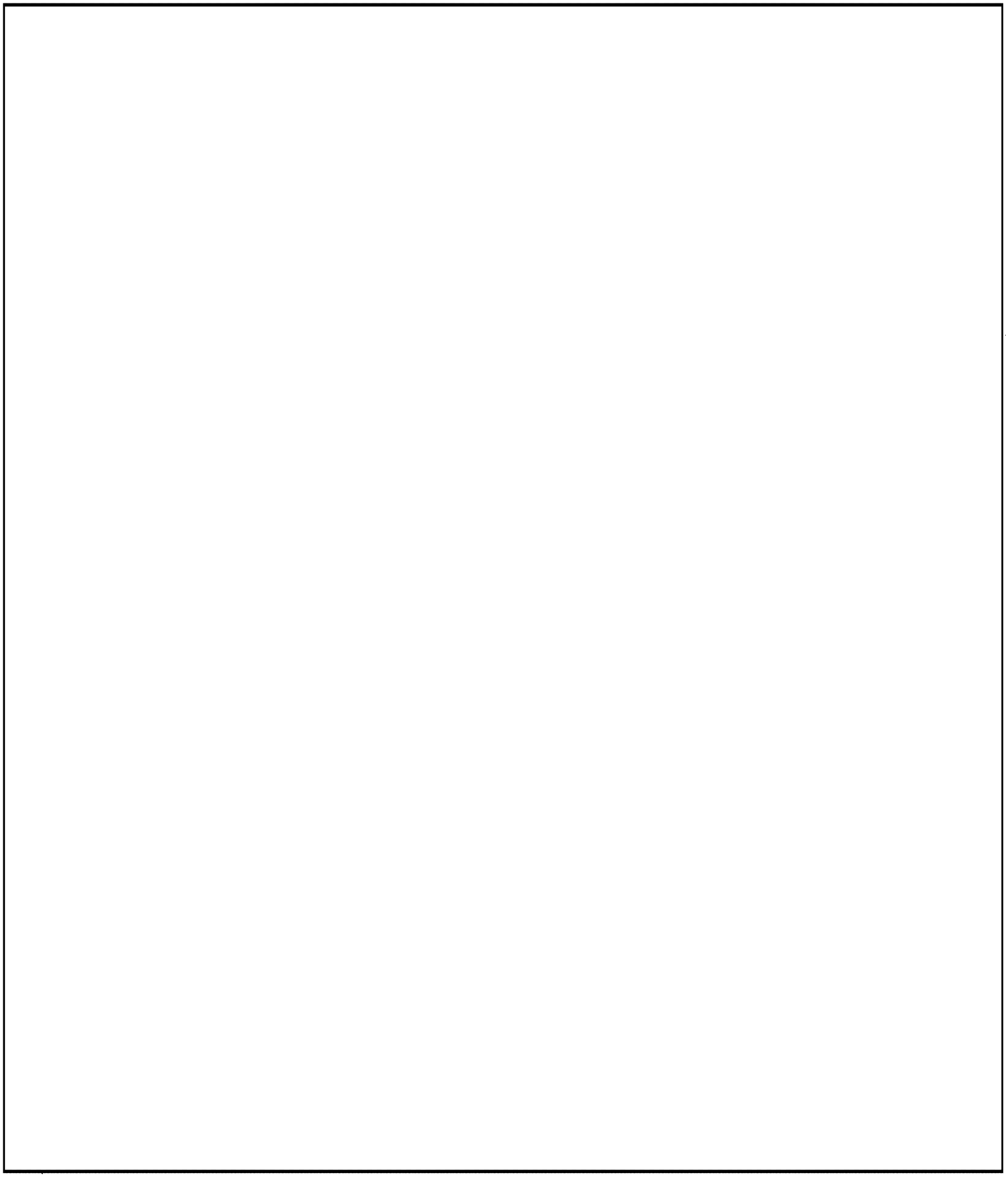
b1 ,b2, b6, b7C, b7E



b1 ,b2, b6, b7C, b7E

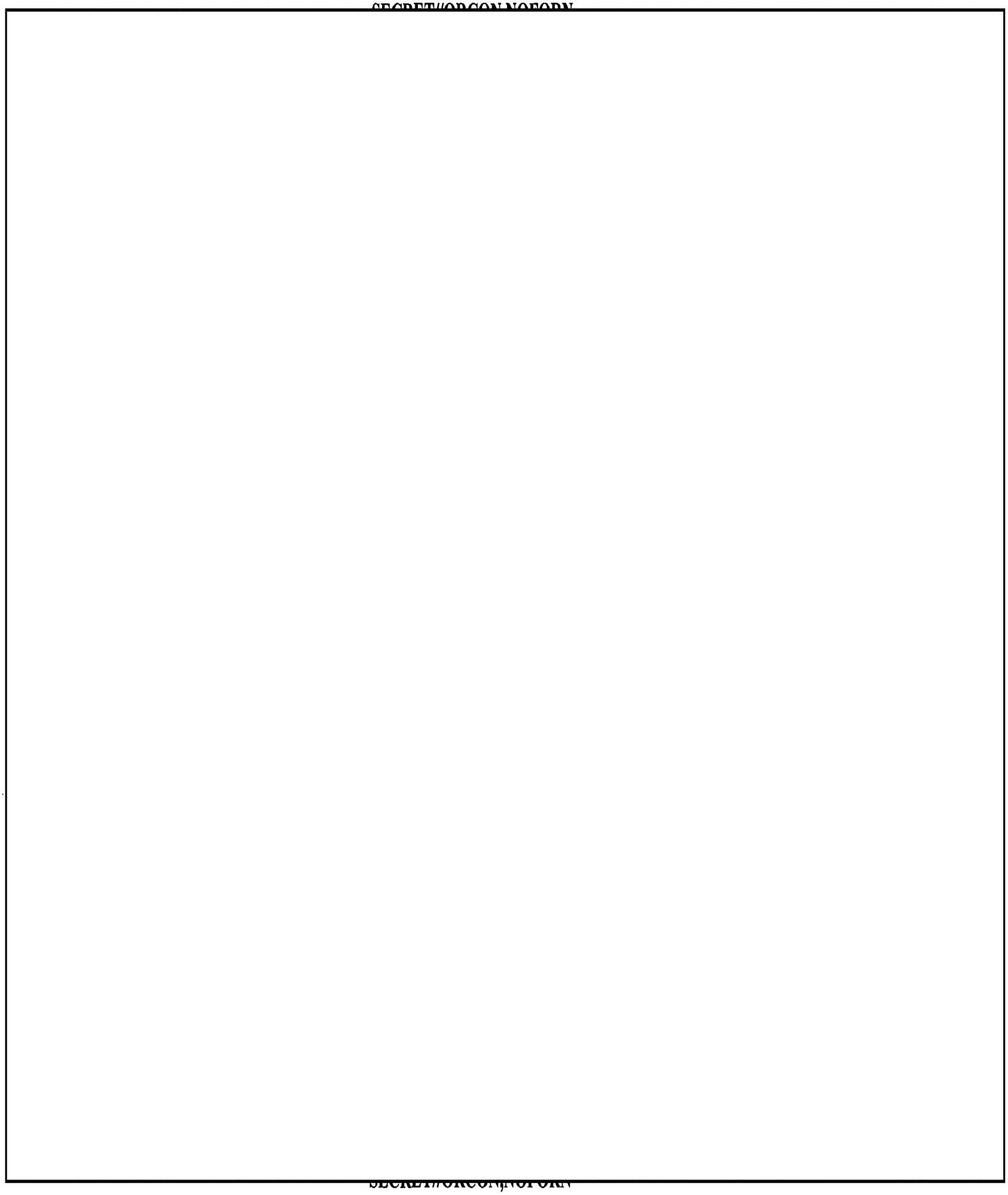


b1 ,b2, b6, b7C, b7E



b1 ,b2, b6, b7C, b7E

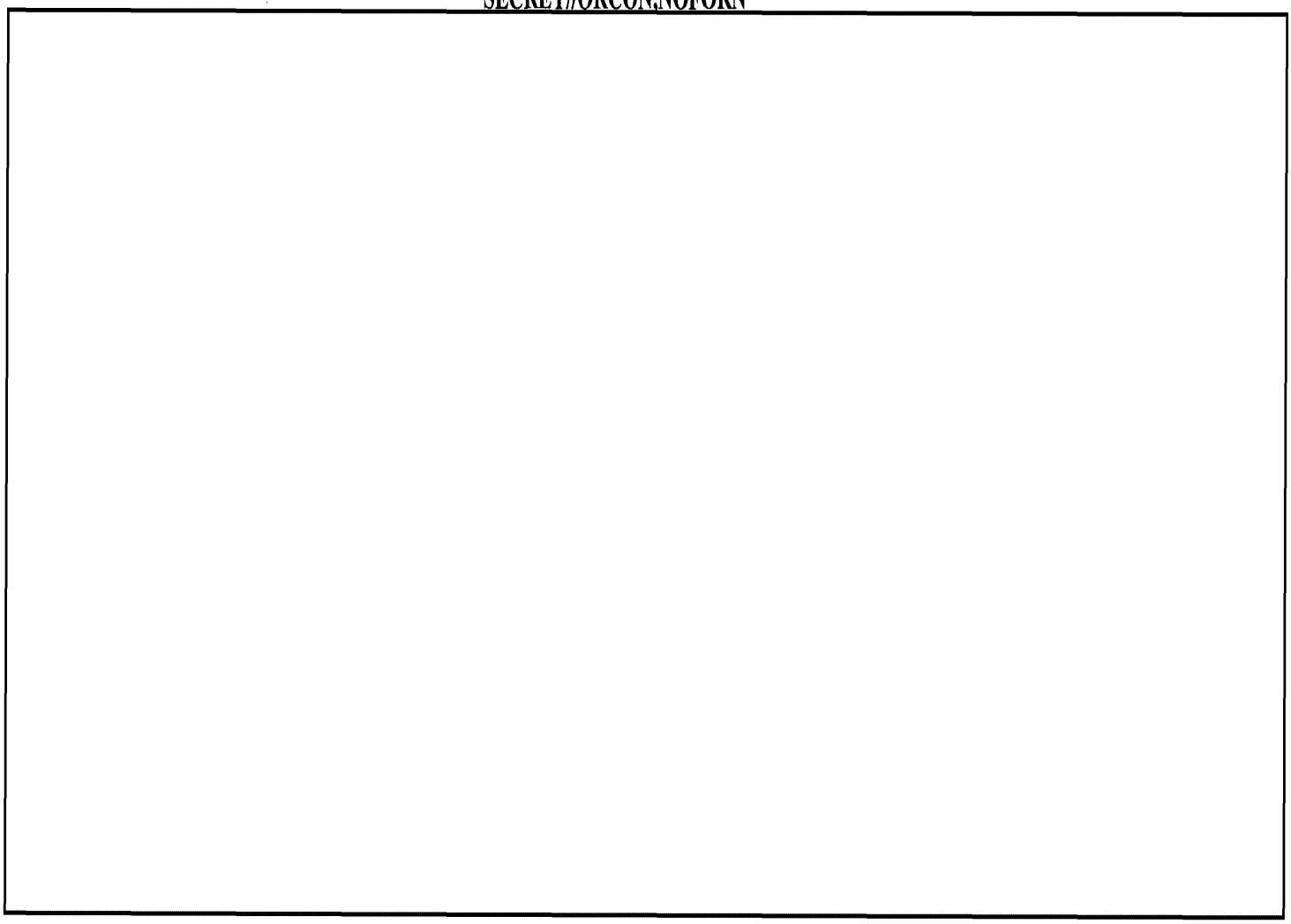
b1 ,b2, b6, b7C, b7E



b1 ,b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E

b1 ,b2, b6, b7C, b7E



b1 ,b2, b6, b7C, b7E

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 227
Page 1 ~ Duplicate
Page 2 ~ Duplicate
Page 3 ~ Duplicate
Page 4 ~ Duplicate
Page 5 ~ Duplicate
Page 6 ~ Duplicate
Page 7 ~ Duplicate
Page 24 ~ Duplicate
Page 25 ~ Duplicate
Page 26 ~ Duplicate
Page 27 ~ Duplicate
Page 28 ~ Duplicate
Page 29 ~ Duplicate
Page 30 ~ Duplicate
Page 32 ~ Duplicate
Page 33 ~ Duplicate
Page 34 ~ Duplicate
Page 35 ~ Duplicate
Page 36 ~ Duplicate
Page 37 ~ Duplicate
Page 38 ~ Duplicate
Page 39 ~ Duplicate
Page 40 ~ Duplicate
Page 41 ~ Duplicate
Page 42 ~ Duplicate
Page 43 ~ Duplicate
Page 44 ~ Duplicate
Page 45 ~ Duplicate
Page 46 ~ Duplicate
Page 50 ~ Duplicate
Page 51 ~ Duplicate
Page 52 ~ Duplicate
Page 53 ~ Duplicate
Page 54 ~ Duplicate
Page 151 ~ Duplicate
Page 152 ~ Duplicate
Page 153 ~ Duplicate
Page 154 ~ Duplicate
Page 155 ~ Duplicate
Page 156 ~ b1, b2, b6, b7C, b7E
Page 157 ~ b1, b2, b6, b7C, b7E
Page 158 ~ b1, b2, b6, b7C, b7E
Page 159 ~ b2, b6, b7C, b7E
Page 160 ~ b2, b6, b7C, b7E

Page 161 ~ Duplicate
Page 162 ~ Duplicate
Page 180 ~ Duplicate
Page 181 ~ Duplicate
Page 182 ~ Duplicate
Page 183 ~ Duplicate
Page 184 ~ Duplicate
Page 185 ~ Duplicate
Page 186 ~ Duplicate
Page 187 ~ Duplicate
Page 188 ~ Duplicate
Page 189 ~ Duplicate
Page 190 ~ Duplicate
Page 191 ~ Duplicate
Page 192 ~ Duplicate
Page 193 ~ Duplicate
Page 201 ~ Duplicate
Page 202 ~ Duplicate
Page 203 ~ Duplicate
Page 204 ~ Duplicate
Page 205 ~ Duplicate
Page 206 ~ Duplicate
Page 208 ~ Duplicate
Page 209 ~ Duplicate
Page 210 ~ Duplicate
Page 213 ~ Referral/Direct
Page 214 ~ Referral/Direct
Page 215 ~ Referral/Direct
Page 216 ~ Referral/Direct
Page 217 ~ Referral/Direct
Page 245 ~ Duplicate
Page 247 ~ Duplicate
Page 248 ~ Duplicate
Page 249 ~ Duplicate
Page 250 ~ Duplicate
Page 251 ~ Duplicate
Page 252 ~ Duplicate
Page 253 ~ Duplicate
Page 254 ~ Duplicate
Page 255 ~ Duplicate
Page 256 ~ Duplicate
Page 257 ~ Duplicate
Page 258 ~ Duplicate
Page 259 ~ Duplicate
Page 260 ~ Duplicate
Page 261 ~ Duplicate
Page 262 ~ Duplicate
Page 263 ~ Duplicate
Page 264 ~ Duplicate
Page 265 ~ Duplicate
Page 266 ~ Duplicate

Page 267 ~ Duplicate
Page 268 ~ Duplicate
Page 269 ~ Duplicate
Page 270 ~ Duplicate
Page 271 ~ Duplicate
Page 272 ~ Duplicate
Page 273 ~ Duplicate
Page 277 ~ Duplicate
Page 278 ~ Duplicate
Page 279 ~ Duplicate
Page 280 ~ Duplicate
Page 281 ~ Duplicate
Page 282 ~ Duplicate
Page 283 ~ Duplicate
Page 284 ~ Duplicate
Page 285 ~ Duplicate
Page 286 ~ Duplicate
Page 287 ~ Duplicate
Page 288 ~ Duplicate
Page 289 ~ Duplicate
Page 290 ~ Duplicate
Page 291 ~ Duplicate
Page 292 ~ Duplicate
Page 377 ~ Duplicate
Page 378 ~ Duplicate
Page 379 ~ Duplicate
Page 380 ~ Duplicate
Page 384 ~ Duplicate
Page 385 ~ Duplicate
Page 386 ~ Referral/Direct
Page 424 ~ Duplicate
Page 425 ~ Duplicate
Page 426 ~ Duplicate
Page 427 ~ Duplicate
Page 428 ~ Duplicate
Page 429 ~ Duplicate
Page 430 ~ Duplicate
Page 431 ~ Duplicate
Page 432 ~ Duplicate
Page 433 ~ Duplicate
Page 434 ~ Duplicate
Page 435 ~ Duplicate
Page 436 ~ Duplicate
Page 437 ~ Duplicate
Page 438 ~ Duplicate
Page 439 ~ Duplicate
Page 440 ~ Duplicate
Page 441 ~ Duplicate
Page 442 ~ Duplicate
Page 443 ~ Duplicate
Page 444 ~ Duplicate

Page 445 ~ Duplicate
Page 446 ~ Duplicate
Page 447 ~ Duplicate
Page 448 ~ Duplicate
Page 449 ~ Duplicate
Page 458 ~ Referral/Direct
Page 459 ~ Referral/Direct
Page 460 ~ Referral/Direct
Page 461 ~ Referral/Direct
Page 462 ~ Referral/Direct
Page 463 ~ Referral/Direct
Page 464 ~ Referral/Direct
Page 465 ~ Referral/Direct
Page 466 ~ Referral/Direct
Page 467 ~ Referral/Direct
Page 468 ~ Referral/Direct
Page 469 ~ Referral/Direct
Page 470 ~ Referral/Direct
Page 471 ~ Referral/Direct
Page 476 ~ Duplicate
Page 477 ~ Duplicate
Page 478 ~ Duplicate
Page 479 ~ Duplicate
Page 481 ~ Duplicate
Page 497 ~ Duplicate
Page 498 ~ Duplicate
Page 499 ~ Duplicate
Page 500 ~ Duplicate
Page 504 ~ Duplicate
Page 505 ~ Duplicate
Page 506 ~ Duplicate
Page 507 ~ Duplicate
Page 508 ~ Duplicate
Page 509 ~ Duplicate
Page 510 ~ Duplicate
Page 511 ~ Duplicate
Page 512 ~ Duplicate
Page 513 ~ Duplicate
Page 514 ~ Duplicate
Page 515 ~ Duplicate
Page 516 ~ Duplicate
Page 517 ~ Duplicate
Page 518 ~ Duplicate
Page 519 ~ Duplicate
Page 520 ~ Duplicate
Page 521 ~ Duplicate
Page 522 ~ Duplicate
Page 523 ~ Duplicate
Page 524 ~ Duplicate
Page 525 ~ Duplicate
Page 526 ~ Duplicate

Page 527 ~ Duplicate
Page 528 ~ Duplicate
Page 529 ~ Duplicate
Page 530 ~ Duplicate
Page 531 ~ Duplicate
Page 532 ~ Duplicate
Page 533 ~ Duplicate
Page 534 ~ Duplicate
Page 535 ~ Duplicate
Page 554 ~ Duplicate
Page 555 ~ Duplicate
Page 558 ~ Duplicate
Page 559 ~ Duplicate
Page 565 ~ Duplicate
Page 566 ~ Duplicate
Page 567 ~ Duplicate
Page 568 ~ Duplicate
Page 569 ~ Duplicate
Page 570 ~ Duplicate
Page 571 ~ Duplicate
Page 572 ~ Duplicate
Page 573 ~ Duplicate
Page 577 ~ Referral/Direct
Page 578 ~ Referral/Direct
Page 579 ~ Referral/Direct
Page 580 ~ Referral/Direct
Page 581 ~ Referral/Direct
Page 582 ~ Referral/Direct
Page 583 ~ Referral/Direct
Page 584 ~ Referral/Direct

[redacted](OGC) (FBI) b6 , b7C

From: [redacted](NK)(FBI) b6 , b7C
Sent: Tuesday, March 22, 2005 11:18 AM
To: [redacted]
Subject: RE:

UNCLASSIFIED

b6 , b7C

NON-RECORD

CDC/ADCs: The article regarding FISA, library records, and the USA Patriot Act, despite containing numerous mistakes about FISA and about the Patriot Act, seems well intentioned and attempts to strike a balance and be fair. The author, Katherine Coolidge, appears to be a law librarian with Bulkley, Richardson, and Gelinas, LLP, and it further appears she may have written the article as an independent study project [redacted] She tries to alleviate the concerns of the American Library Association and finds fault with several provocative and incorrect statements made by ALA Associate Executive Director Emily Sheketoff. She also clearly takes exception, as well, to several provocative statements made by former AG Ashcroft, especially those statements he made in a speech before the National Restaurant Association, where he derisively dismissed the concerns of librarians regarding FBI use of the FISC to obtain library records. b6 b7C

Her many inaccurate statements regarding FISA and the FISC seem to have been obtained from her interview with Kevin O'Connor, US Attorney for the District of Connecticut. According to one of Coolidge's footnotes, John Danaher, an AUSA in the District of Connecticut who specializes in foreign intelligence investigations, participated with Mr. O'Connor in the interview. So that might be why she got some things correct. At any rate, despite the many errors the article should alleviate the concerns of librarians that the FBI is using FISA to obtain library records, and also to emphasize that the FISC is not a rubber stamp for FBI surveillance.

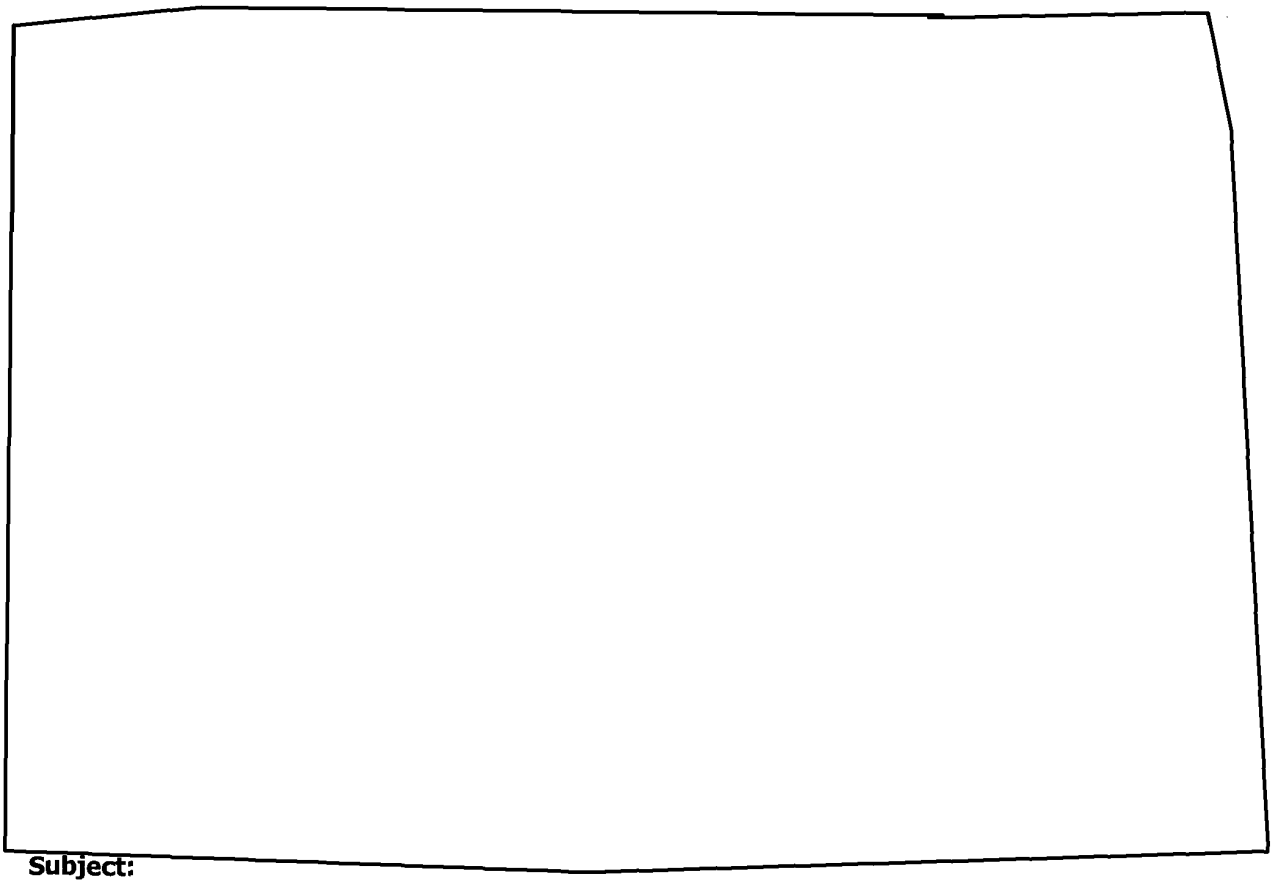
In summary, her two human sources of information regarding FISA were people (Sheketoff and O'Connor) that don't know too much about FISA (especially Sheketoff). Mr. O'Connor might know more about FISA, and Coolidge may just have gotten it wrong. I'll end with two quotes from Coolidges article:

"Misinformation is destructive and undermines the security of everyone."

"While a wholesale abdication of civil rights without question would be absurd, so too is an alarmist mispresentation of information about the operation of the USA PATRIOT Act and the FISC process."

CDC [redacted]
Newark b6 , b7C

-----Original Message----- b6 , b7C
From: [redacted] (OGC) (FBI)
Sent: Monday, March 21, 2005 11:54 AM
To: [redacted]



Subject:

UNCLASSIFIED
NON-RECORD

b6 , b7C

UNCLASSIFIED

UNCLASSIFIED

b6 , b7C

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6

Sent: Monday, January 10, 2005 4:04 PM b7C

To: [redacted] (OGC) (FBI)

Subject: RE: tax information

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-15-2005 BY 65179DMH1r2 Ca#05-CV-0845

UNCLASSIFIED
NON-RECORD

Thanks!

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, January 10, 2005 4:01 PM
To: [redacted] (OGC) (FBI)
Subject: RE: tax information

b6
b7C

b3 /FGJ
b5

UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

pik

b3 /FGJ
b5

-----Original Message-----
From: [redacted] (OGC) (FBI)
Sent: Monday, January 10, 2005 3:46 PM
To: [redacted] (OGC) (FBI)
Subject: FW: tax information

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b3 /FGJ
b6
b7C

Here's more info re that tax issue we discussed last week. [redacted] See below. What do you think? Thanks for your help.

[redacted]

-----Original Message-----
From: [redacted] (DE) (FBI)
Sent: Monday, January 10, 2005 3:20 PM
To: [redacted] (OGC) (FBI)

b6
b7C

Cc: [redacted](DE) (FBI) b6 b7C
Subject: RE: tax information

UNCLASSIFIED
NON-RECORD

b6 , b7C

[redacted]

Forgive me for my ignorance, and thanks for the follow-up - I really appreciate it! [redacted]

b3 /FGJ
b5
b6
b7C

[redacted]

[redacted]

[redacted]

Thanks,

[redacted]

b6 , b7C

b3 /FGJ
b5
b6
b7C

-----Original Message-----
From: [redacted](OGC) (FBI) b6 b7C
Sent: Friday, January 07, 2005 2:47 PM
To: [redacted](DE) (FBI)
Subject: FW: tax information

UNCLASSIFIED
NON-RECORD

b6 , b7C [redacted] See below regarding your question. Does that help at all?

[redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, January 07, 2005 2:43 PM b6 b7C
To: [redacted](OGC) (FBI)
Subject: RE: tax information

UNCLASSIFIED
NON-RECORD

b5 [redacted]

pik

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, January 07, 2005 2:36 PM
To: [redacted](OGC) (FBI)
Subject: RE: tax information

b6
b7C

UNCLASSIFIED
NON-RECORD

b5
b6
b7C

Thanks [redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, January 07, 2005 12:15 PM
To: [redacted](OGC) (FBI)
Subject: tax information

b6
b7C

UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted] 26 USC 6301(i)(1)(A), Disclosure to federal officers or employees for administration of federal laws not relating to tax administration - **disclosure of returns and return information for use in crminal investigations** -- provides that
"any return or return information with respect to any specified taxable period or periods shall, pursuant to and upon the grant of an ex parte order by a federal district court judge or magistrate under subparagraph (B) [which describes the application that needs to be filed] be open (but only to the extent necessary as provided in such order) to inspection by, or disclosure to, officers and employees of any federal agency who are personally and diretly engaged in:
(i) preparation for any judicial or adminsitrative proceeding pertaining to the enforcement of a specifically designated Fedearl criminal statute (not involving tax administration) to which the US or such agency is or may be a party,
(ii) any investigation which may result in such a proceeding, or
(iii) any federal grand jury proceeding pertaining to enforcement of such a criminal statute to which the US or such agency is or may be a part,

solely for the use of such officers and employees in such preparation, investigation, or grand jury proceeding.

(B) discusses the procedures and says that upon application by a prosecutor, the judge or magistrate may grant the order if he determines that
"(i)there is reasonable cause to believe, based upon information believed to be reliable, that a specific criminal act has been comitted,
(ii) there is reasonable cause to believe that the return or return information is or may be relevant to a matter relating to the commission of such act, and
(iii) the return or return information is sought exclusively for use in a federal criminal investigation or proceeding concerning such act, and the information sought to be disclosed cannot reasonably be obtained, under the circumstances, from another source."

[redacted]

b5

b5

[redacted]

b5

[redacted]

pik

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 02/27/2004

To: All Field Offices **Attn:** SAC/ADIC
FBIHQ, Manuals Desk

All Legats **Attn:** Legat

Counterterrorism **Attn:** AD Gary Bald

Criminal Investigative **Attn:** AD Grant D. Ashley

Cyber **Attn:** AD Jana D. Monroe

Counterintelligence **Attn:** AD David W. Szady

b2
b6
b7C

From: Office of the General Counsel
Investigative Law Unit/Room 7326
Contact: [redacted]

Approved By: Caproni Valerie E VC
Curran John JPC
Kelley Patrick W PWK
[redacted]

b6
b7C

Drafted By: [redacted]

Case ID #: ~~66F-HQ-C134260 (Pending)~~ 66F-HQ-1364260-5
66F-HQ-C1384970 -7564

Title: USA PATRIOT Act
Sunset Provisions

Synopsis: Many of the investigative tools created by the USA PATRIOT Act will sunset or expire on December 31, 2005 unless Congress acts otherwise. Details on the use of these tools are necessary to assist in justifying the continued need for these investigative tools. Offices are to provide the Investigative Law Unit, Office of the General Counsel (OGC) with statistics, good examples, or, at the very least, a brief narrative summarizing the benefits the office has received from these provisions by March 19, 2004.

Reference: 66F-HQ-1085160- Serial 57

Details: The USA Patriot Act contained numerous provisions which are scheduled to sunset on December 31, 2005 unless Congress acts otherwise. The DOJ and the FBI are now beginning the process of gathering evidence to demonstrate the use of these investigative tools. Specific instances where these provisions were of assistance to achieve investigative or prosecutorial goals will be instrumental in securing their renewal. For this reason, in June of 2002, when the OGC issued guidance on the provisions addressing investigative issues (see above referenced EC), it encouraged offices to keep records of the effective use of these tools. The EC also stated

that "important information to be maintained includes both the number of times the investigative tool was effectively used and specific information on noteworthy cases." This type of information will be critical in defending the need for these tools. If we do not take the time to set forth a strong defense complete with real examples of the effectiveness of these tools, Congress may let some or all of these investigative tools expire, thus reducing our arsenal against terrorism and other serious crimes.

In this regard, offices are requested to provide statistics, good examples, or, at the very least, a brief narrative summarizing the benefits the office has received from these provisions. The information should be forwarded to the Investigative Law Unit, Office of the General Counsel (Room 7326) by **March 19, 2004.** Thereafter, offices are encouraged to continue providing the Investigative Law Unit new information on the use of these provisions as it becomes available. Many of the provisions scheduled to sunset are described below. Additional information is available on each provision as noted in the description below or in the above referenced EC.

Voice Mail - Section 209 of the Act enabled law enforcement to obtain all voice mail which is stored by a communications provider, including unopened voice mail, using the procedures set forth in 18 U.S.C. §2703 (such as a search warrant). This also applies to other wire communications as defined by the statute. Voice messages stored and in the possession of the user, such as messages on an answering machine, are not covered by this statute. [redacted] b5 [redacted] See 18 U.S.C. § 2510; 18 U.S.C. § 2703.

Nationwide Search Warrants for E-mail and Associated Records - Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

Voluntary Disclosures - Section 212 of the law explicitly permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers. This provision also allows a communications service provider to disclose non-content records to protect their rights and property. This portion of the provision will most often be used when the communications service provider itself is a victim of computer hacking. See 18 U.S.C. § 2702(b) & (c)(3); 18 U.S.C. § 2703(c)(2)(F).

For about ten months (January 2003-November 2003) there was a mandatory reporting requirement for the receipt of content information (usually e-mail content) under this emergency disclosure provision. (See the Homeland Security Act and EC 66F-HQ-C1384970 Serial 501.) During that time, offices were only required to report the number of e-mail messages that were received under this voluntary disclosure provision. Offices were not required to report the receipt of records and were also not required to provide case information. For this reason, it would be beneficial for offices to now report more detail on these voluntary

disclosures. Examples where voluntary disclosures led to valuable foreign intelligence or arrests would be particularly helpful.

Information Sharing - Section 203(b) & (d) of the Act provided new information sharing capabilities between criminal and intelligence investigations for foreign intelligence information and information obtained via a Title III electronic surveillance. (See EC 66F-HQ-A1247863-71 dated 10/26/01 for additional information.) Recognizing that this tool has become a regular part of how the FBI operates, especially in terrorism cases, no statistics are necessary. However, case examples that demonstrate the importance of this tool should be provided.

Intercepting Communications of Computer Trespassers - Section 217 of the Act clarified an ambiguity in the law by explicitly providing victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. Before monitoring can occur, however, four requirements must be met. First, consent from the owner or operator of the protected computer must be obtained. Second, law enforcement must be acting pursuant to an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation. Third, law enforcement must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. And fourth, investigators must only intercept the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting authorized users. Additionally, based on the definition of a "computer trespasser," communications of users who have a contractual relationship with the computer owner may not be monitored, even if their use is in violation of their contract terms (i.e. spammers). See 18 U.S.C. § 1030(e)(2); 18 U.S.C. § 2510 (20) & (21); 18 U.S.C. § 2511(2)(i).

Expanded Predicates for Title III - Sections 201 & 202 of the Act expanded the predicate offenses for Title III to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). See 18 U.S.C. § 2516.

Roving FISA Surveillance - Section 206 amended FISA to allow the Court to issue a "generic" secondary order where the Court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person." This means that, when a FISA target engages in trade craft designed to defeat electronic surveillance, such as by rapidly switching cell phones, Internet accounts, or meeting venues, the Court can issue an order directing "other persons," i.e., the as yet unknown cell phone carrier, Internet service provider, etc., to effect the authorized electronic surveillance. Even if the target is not engaged in obvious trade craft, we can obtain such an order as long as the target's actions may have the effect of thwarting surveillance. This allows the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. For additional information see EC 66F-HQ-A1247863-71 dated 10/26/01. Any examples where roving authority has been obtained and utilized to gain valuable foreign intelligence should be provided.

New Standard for FISA Pen/Trap - Section 214 of the Act eliminated the requirement that the FISA pen/trap order include specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in

communications with such an agent, under specified circumstances. FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." For additional information see EC 66F-HQ-A1247863-71 dated 10/26/01.

Changes to "Primary Purpose" Standard for FISA - Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." [redacted] b5 [redacted] For additional information see EC 66F-HQ-A1247863 Serial 71 dated 10/26/01. While no statistics are required for this provision, case examples and brief narratives on the benefits of this provision are sought.

New Standard for Business Records under FISA - Section 215 changed the business records authority found in Title V of FISA. The old language allowed the FISA Court to issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articulable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. Section 215 changed this standard to simple relevance (just as in the FISA pen register standard described above) and gave the Court the authority to compel production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This is the same standard described above for Section 214. For additional information see EC 66F-HQ-A1247863-71 dated 10/26/01.

All submissions should be made via EC to the attention of [redacted] Investigative Law Unit, Office of the General Counsel, FBIHQ Room 7326 by **March 19, 2004**. Questions should be directed to either Assistant General Counsel [redacted] or Unit Chief [redacted]

b2
b6
b7C

To: All Field Offices From: Office of the General Counsel
Re: 66F-HQ-C134260, 02/27/2004

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Offices are to provide the Investigative Law Unit, Office of the General Counsel (OGC) with statistics, good examples or anecdotes, or at the very least, a brief narrative summarizing the benefits the office has received from these provisions by **March 19, 2004.**

CC: Ms. Caproni
Mr. Kelley
Mr. Curran
[redacted]
ILU - 2

b6
b7C

♦♦

INFORMAL NOTE -FOR RETENTION

11/9/2004

To: ALL NSLB Employees

RE: PROCESSING OF ALL BUSINESS RECORDS
ORDERS UNDER 50 U.S. C. 1861

After receiving a business records request (215 requests) from the field, NSLB will review the request to determine if it meets the requirements of law, prepare an application, and proposed order, and, in addition, review the request to determine if any other federal statute arguably governs the release of the records sought. If the NSLB attorney determines no other federal statute arguably governs the release of the records sought as is the case with hotel records and telephone records, a brief memorandum to OIPR detailing this conclusion should be attached to the package prior to submitting the package to OIPR. Upon receipt of these "simple" 215s, OIPR will endeavor to review and approve them for presentation to the FISC within 48 hours. Further, if a problem with the package surfaces, OIPR will use its best efforts to voice its legal objection and suggest solutions within this same 48 hour time frame. It is contemplated that these "simple" requests should occasion few, if any, edits for style.

If the NSLB attorney determines that another federal statute arguably governs the release of the records sought, he or she should prepare a detailed memorandum outlining what statutes might apply, their scope with respect to release, and the attorney's conclusion as to whether 50 U.S.C. 1861 is controlling and will authorize release. This memorandum should be reviewed with the NSLB attorney's unit chief. If it appears release is not authorized, a letter for my signature should be prepared explaining our legal reasoning for dissemination to the requesting field office.

If it is the legal opinion of the NSLB attorney and the unit chief that release of the requested records is authorized, the legal memorandum should be forwarded to OIPR with the request for the 215 order. OIPR will use its best efforts to process these requests expeditiously as well; however, it is understood that these requests requiring, as they do, more extensive analysis may take more time. As a track record for these requests develops, I will coordinate with OIPR as necessary to address issues of concern or timeliness.

This process will need refinement over time. Please forward any suggestions you may have for improvement to your unit chiefs or to me directly.

Julie F. Thomas

CC: Margaret Skelley-Nolan, OIPR
James A. Baker, OIPR

Patriot Act II - Lyg Proposals

b6
b7C

Copy

MEMORANDUM TO:

FROM: FBI-OGC

SUBJECT: Comments on 1-9-03 Draft of Domestic Security Enhancement Act

DATE: January 14, 2003

b5

limited

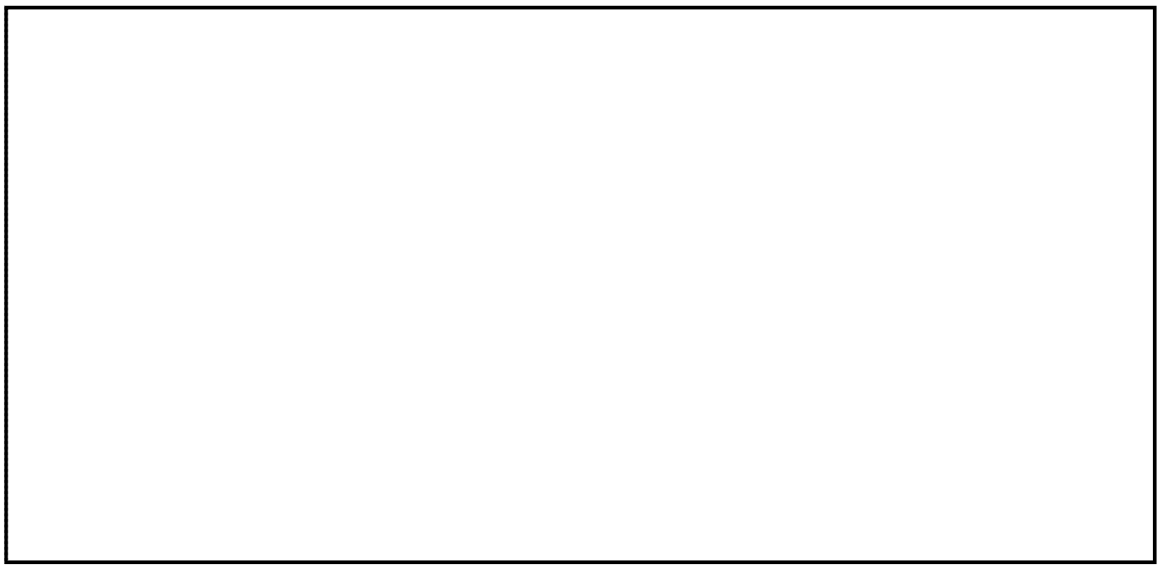
50 USC 186

Additional Comments:

b5

b6

b7C



b5

November 15, 2002

FBI Terrorism Legislation Proposals

1. **National Security Law Proposals**

INFORMATION SHARING

[redacted] b5

INVESTIGATIVE TECHNIQUES

[redacted] b5

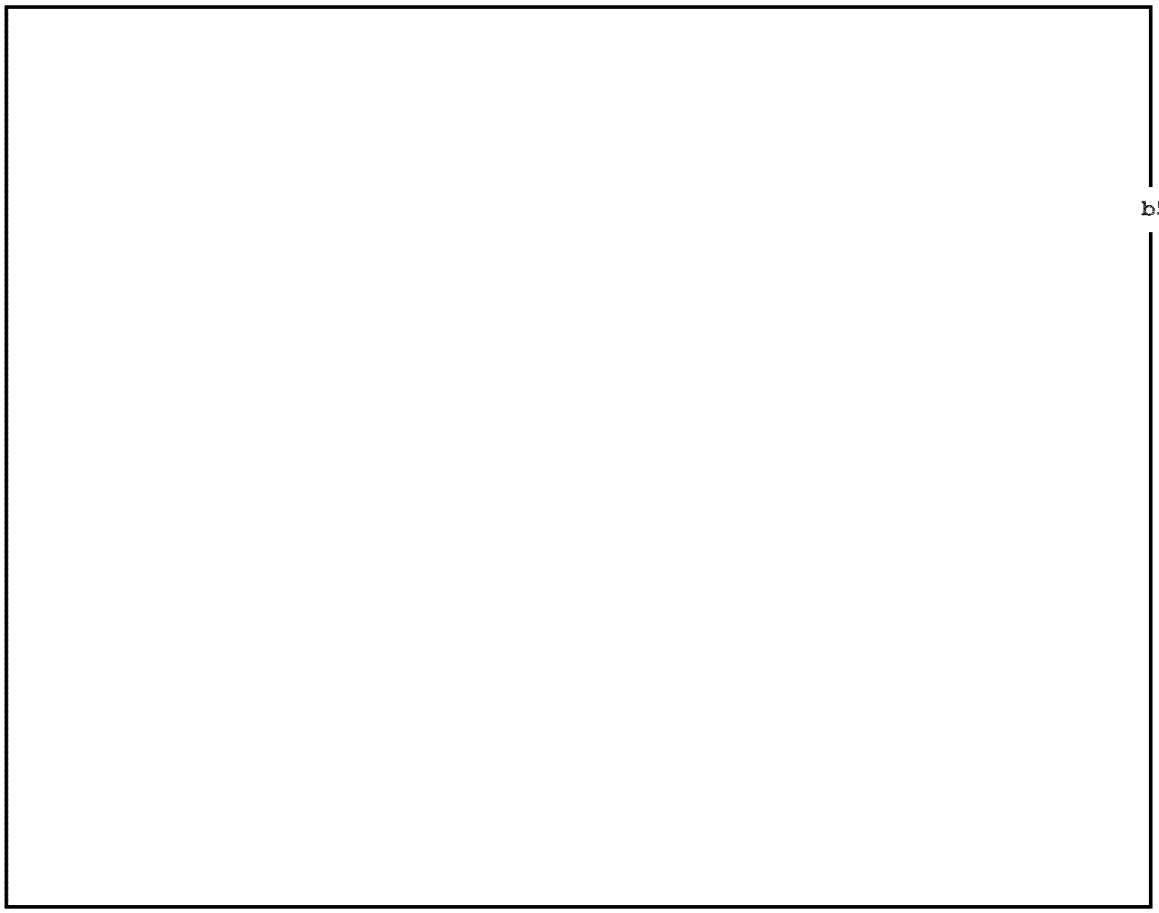
[redacted] b5

[redacted] b5

[redacted] b5

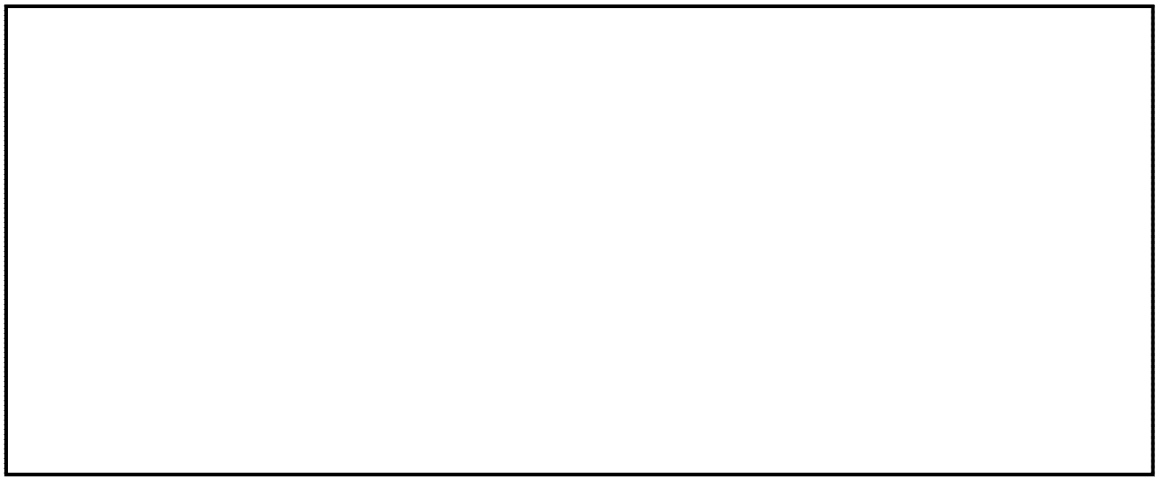
[redacted] b5

[redacted] b5



b5

FISA



b5

[redacted] b5

[redacted] b5

[redacted] b5

[redacted] b5

[redacted] b5

2. **Privacy Act/FOIPA Proposals**

A. Amend the Privacy Act as follows:

A BILL

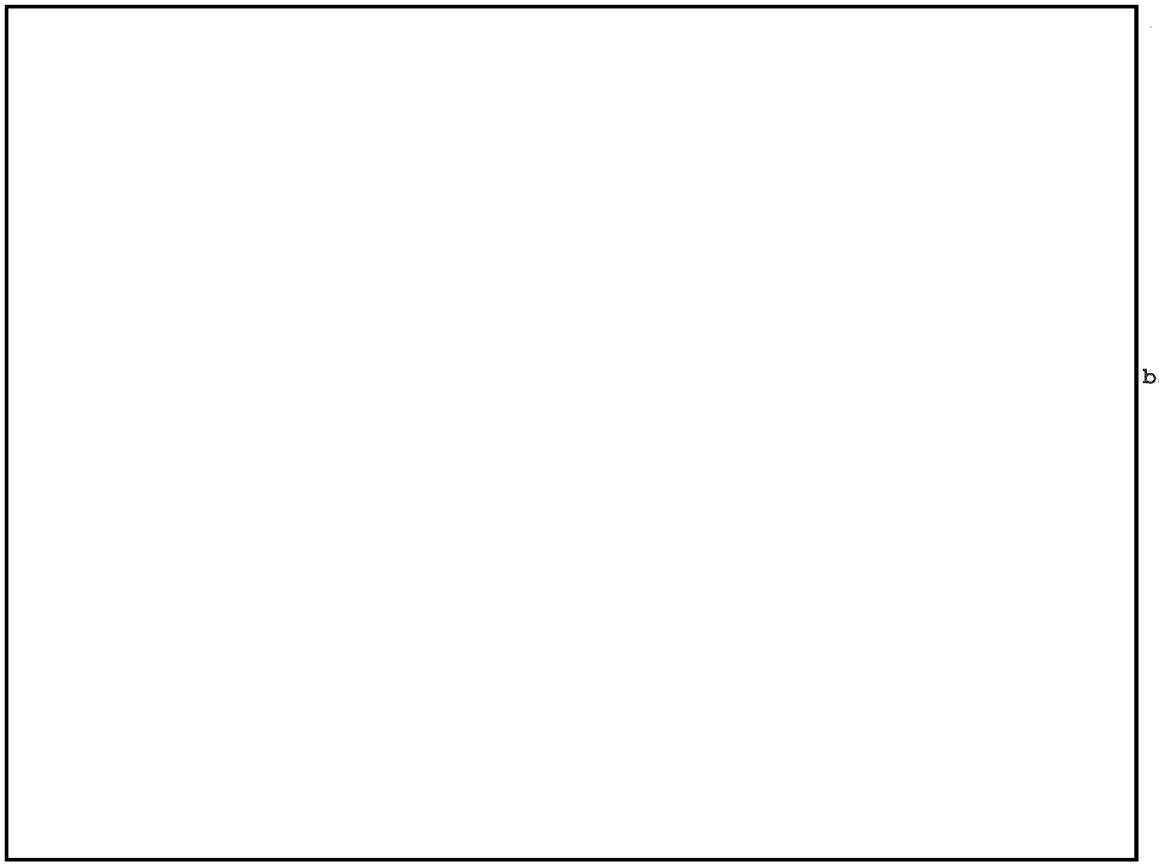
[redacted] b5

SECTION 1. SHORT TITLE

[redacted] b5

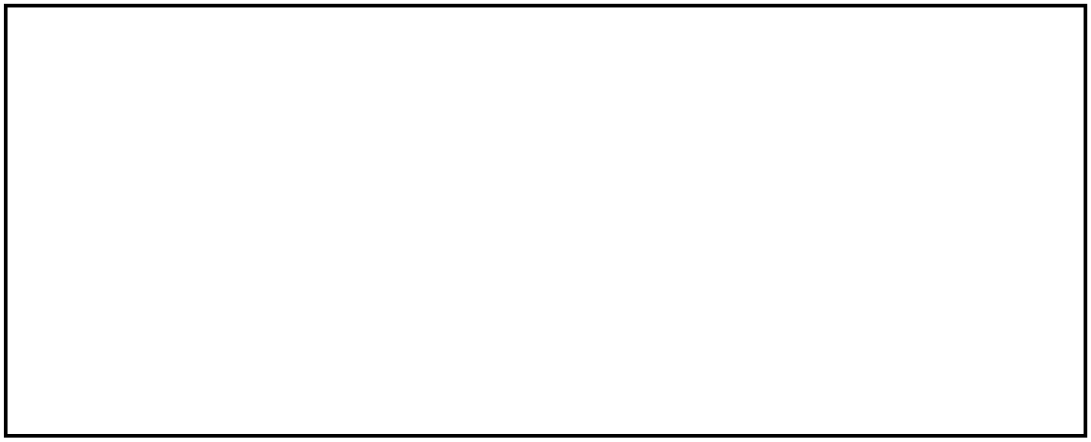
SECTION 2. PROTECTING SENSITIVE LAW ENFORCEMENT AND NATIONAL SECURITY RECORDS FROM DISCLOSURE

[redacted] b5



b5

SECTION 3. AUTHORITY TO OBTAIN OFFICIAL INFORMATION

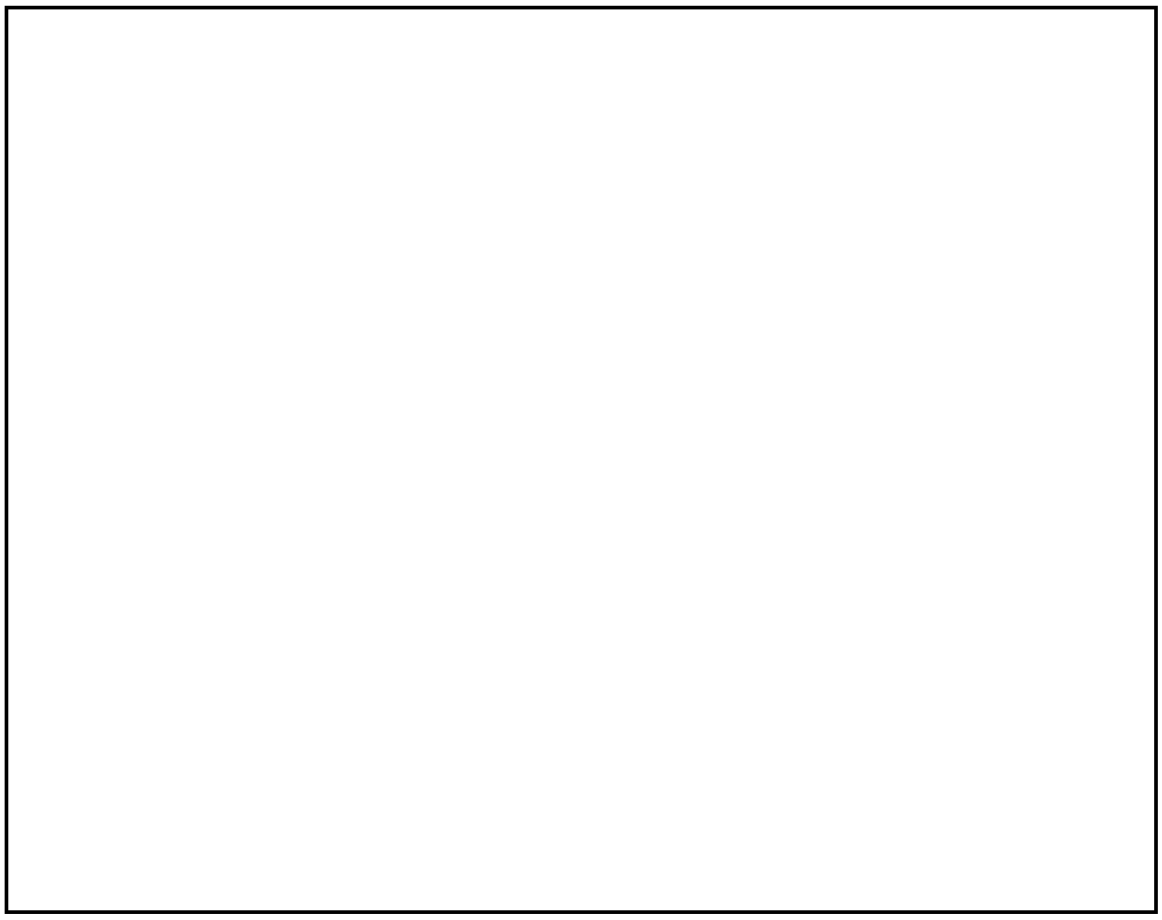


b5

SECTION-BY-SECTION ANALYSIS OF THE PROPOSED AMENDMENTS
TO THE PRIVACY ACT

[redacted] b5

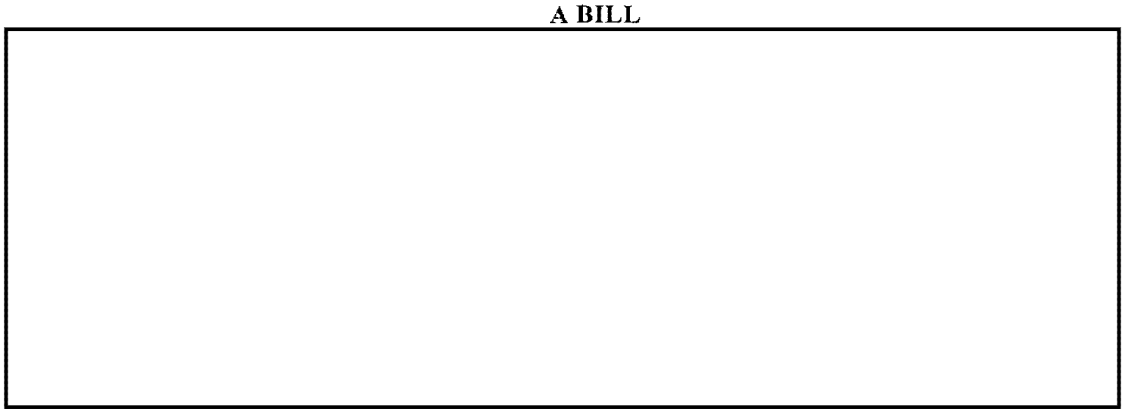
[redacted] b5



b5

B. Amend FOIPA as follows:

A BILL



b5

SECTION 2. PROHIBITING FREEDOM OF INFORMATION ACT REQUESTS BY FOREIGN PERSONS AND SUSPECTED TERRORISTS

[redacted] b5

SECTION 3. PRESERVING THE USE OF EXEMPTIONS

[redacted] b5

SECTION 4. DELAYED DISCLOSURE OF SENSITIVE TECHNICAL DATA

[redacted] b5

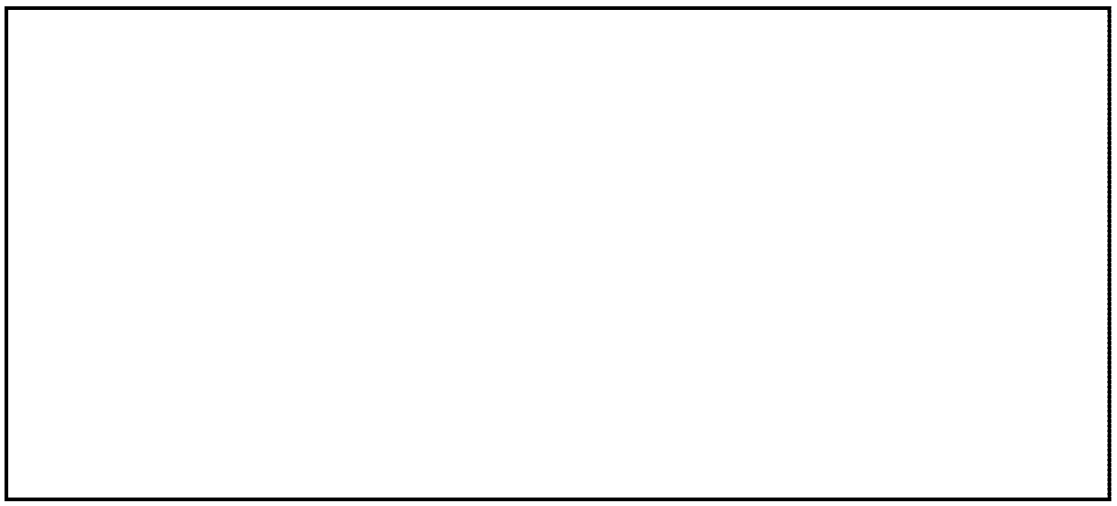
[redacted] b5

SECTION 5. PROTECTING SENSITIVE LAW ENFORCEMENT RECORDS FROM DISCLOSURE

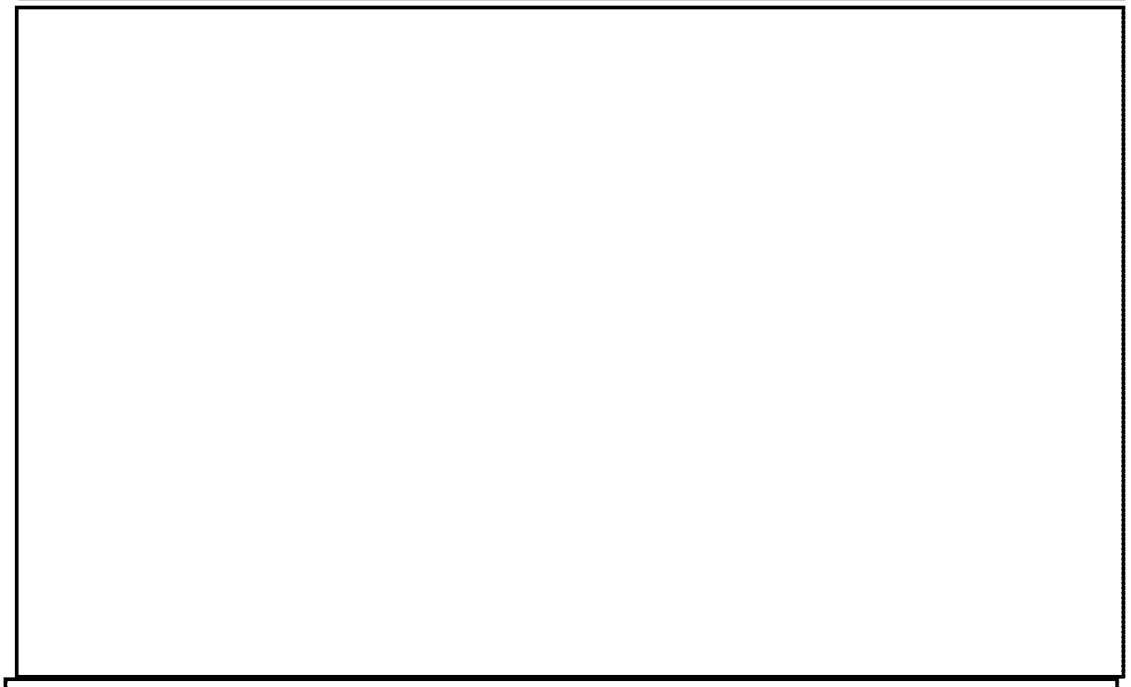
[redacted] b5

SECTION-BY-SECTION ANALYSIS OF THE PROPOSED AMENDMENTS TO THE FREEDOM OF INFORMATION ACT

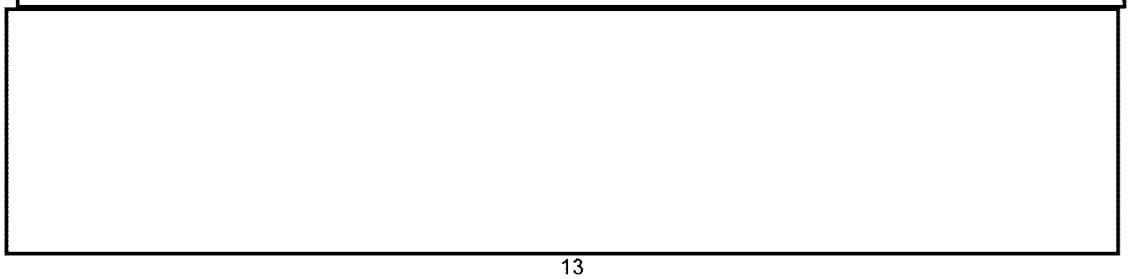
[redacted] b5



b5



b5



b5

[redacted] b5

3. **Amend the National Crime Prevention and Privacy Compact Act of 1998**

[redacted] b5

4. **Amend CALEA (Communications Assistance for Law Enforcement Act)**

[redacted] b5

[redacted] b5

2.

SEC. 107. TECHNICAL REQUIREMENTS AND STANDARDS; EXTENSION OF COMPLIANCE DATE.

[redacted] b5

* * * * *

[redacted] b5

* * * * *

[redacted] b5

[redacted] b5

3.

SEC. 108. ENFORCEMENT ORDERS.

[redacted] b5

* * * * *

[redacted] b5

4.

SEC. 102. DEFINITIONS.

[redacted] b5

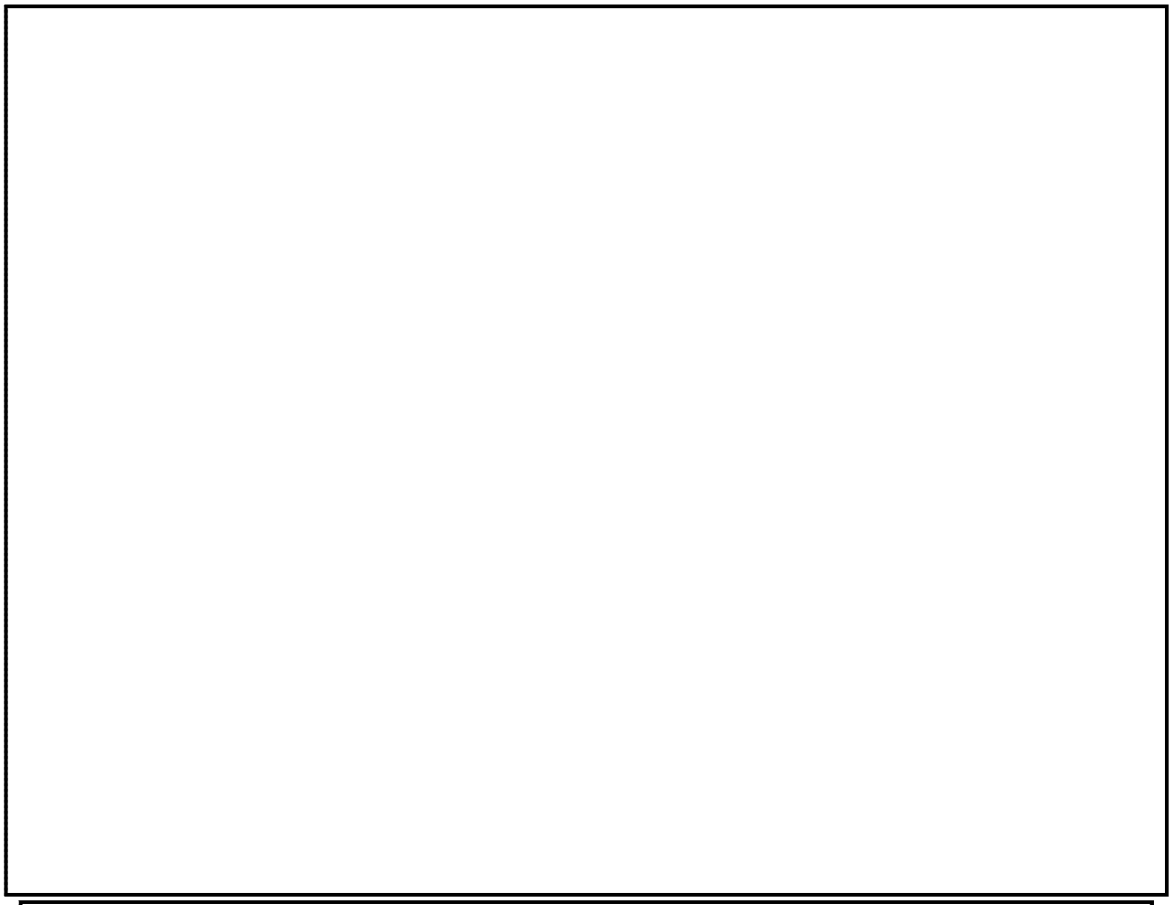
[redacted] b5

[redacted] b5

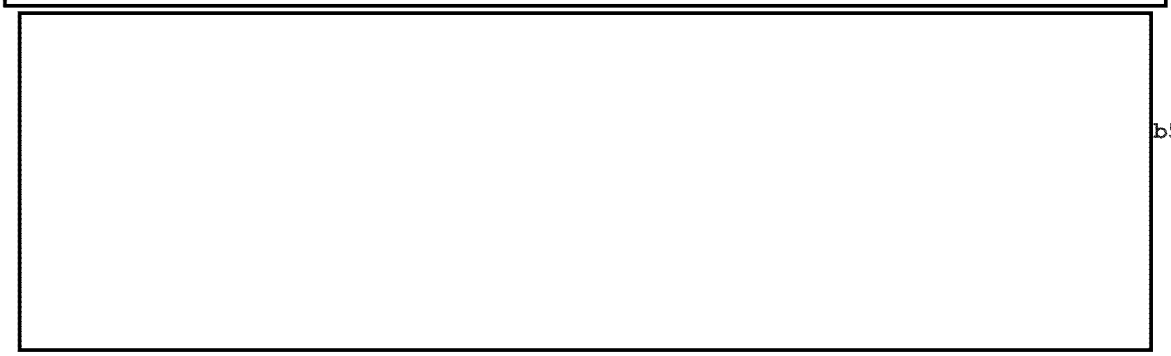
[redacted] b5

SEC. 103. ASSISTANCE CAPABILITY REQUIREMENTS.

[redacted] b5

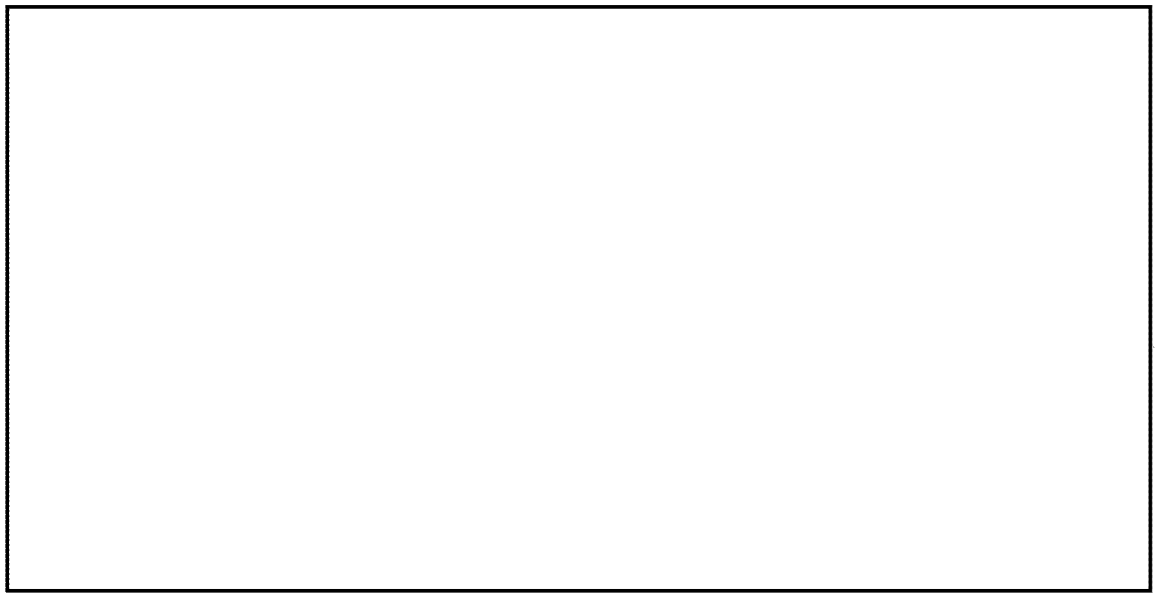


b5



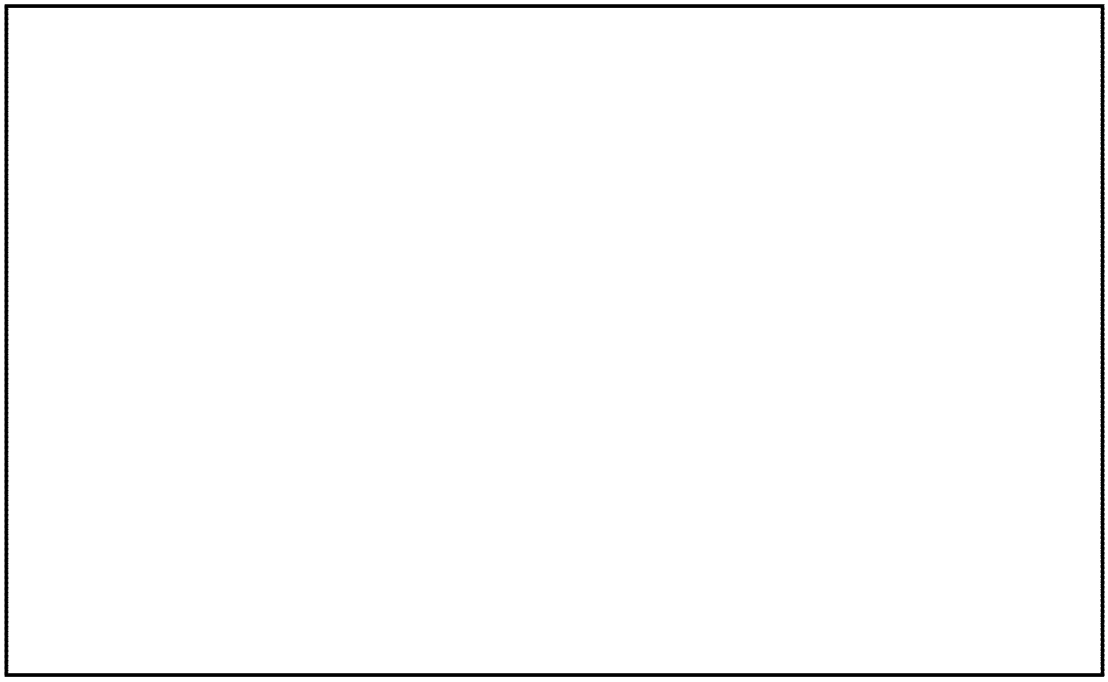
b5

* * * * *



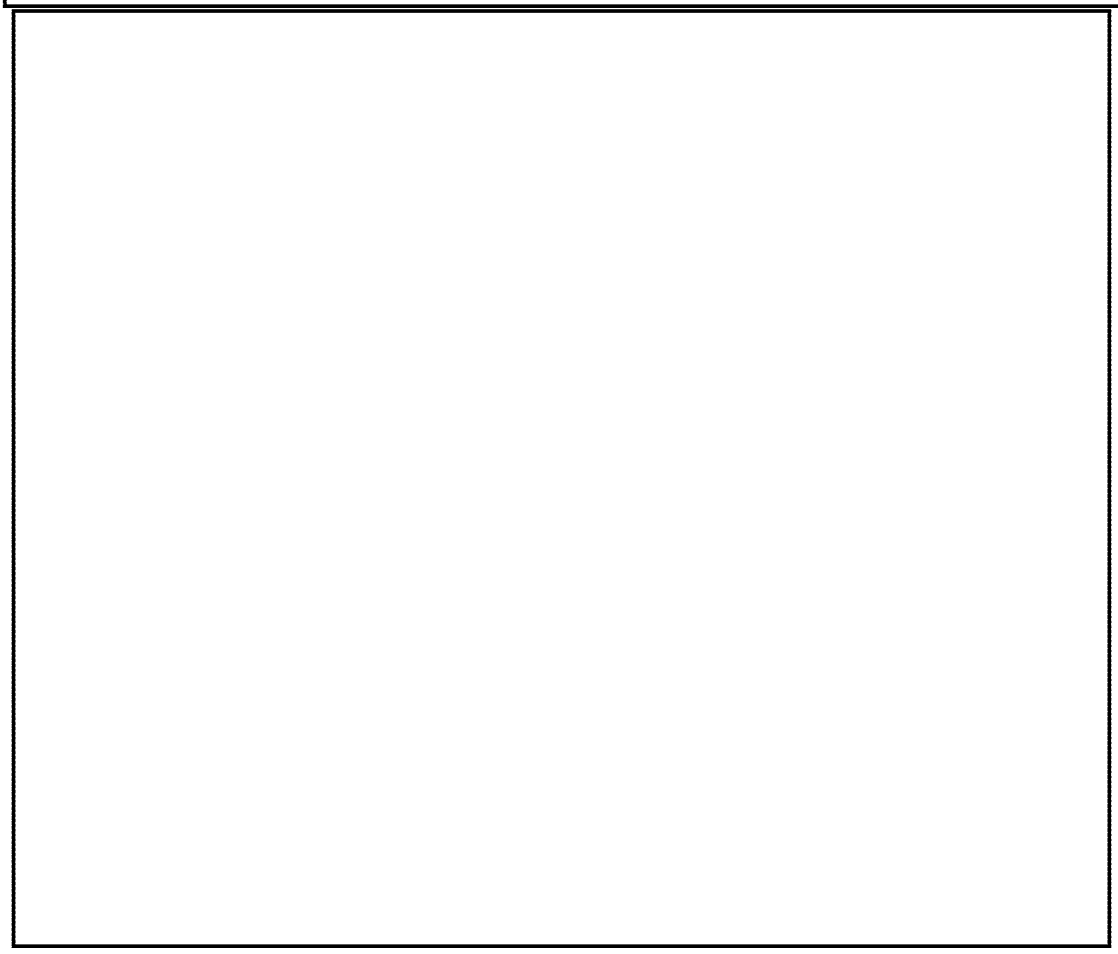
b5

* * * * *



b5

b5



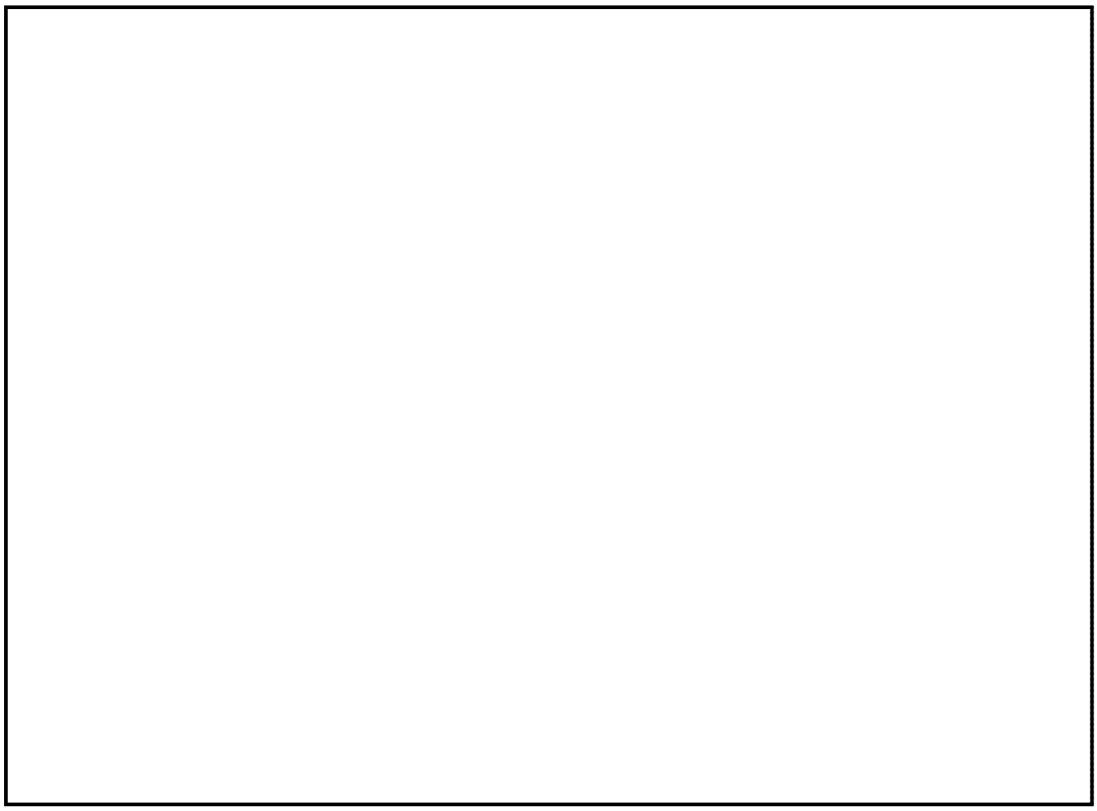
b5

[redacted] b5

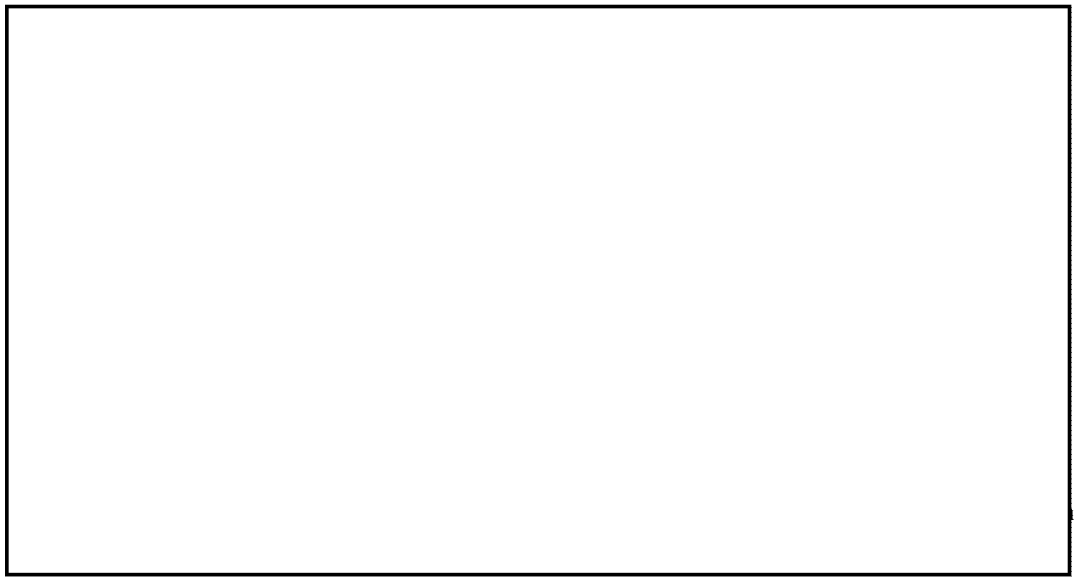
[redacted] b5

5. **Other Proposals**

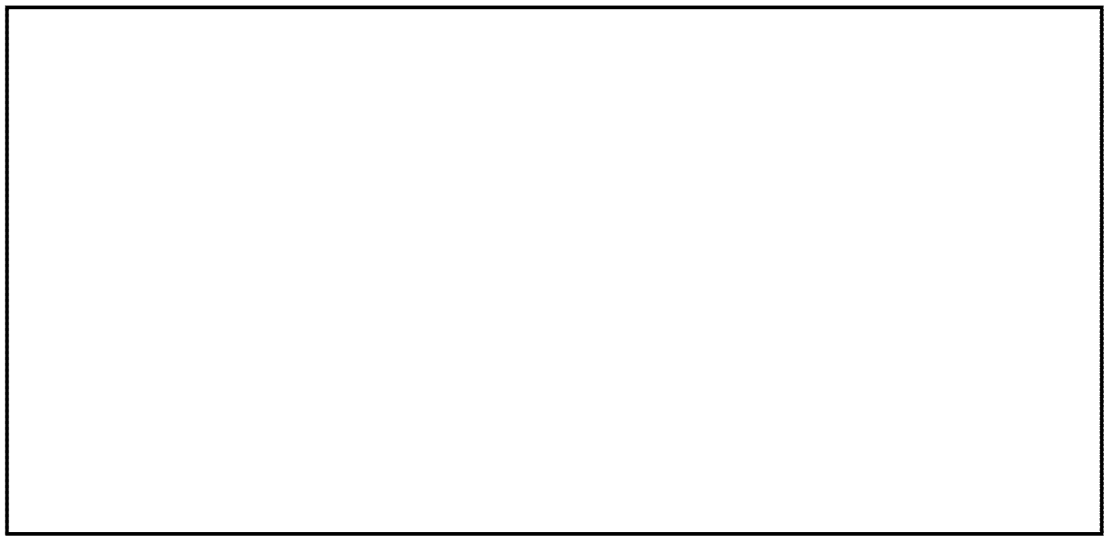
[redacted] b5



b5



b5



b5

CONFIDENTIAL—NOT FOR DISTRIBUTION
Draft—January 9, 2003

DOMESTIC SECURITY ENHANCEMENT ACT OF 2003

SECTION-BY-SECTION ANALYSIS

Title I: Enhancing National Security Authorities

Subtitle A: Foreign Intelligence Surveillance Act Amendments

Section 101: Individual Terrorists as Foreign Powers.

Under 50 U.S.C. § 1801(a)(4), the definition of "foreign power" includes groups that engage in international terrorism, but does not reach unaffiliated individuals who do so. As a result, investigations of "lone wolf" terrorists or "sleeper cells" may not be authorized under FISA.

[redacted] b5

Section 102: Clandestine Intelligence Activities by Agent of a Foreign Power.

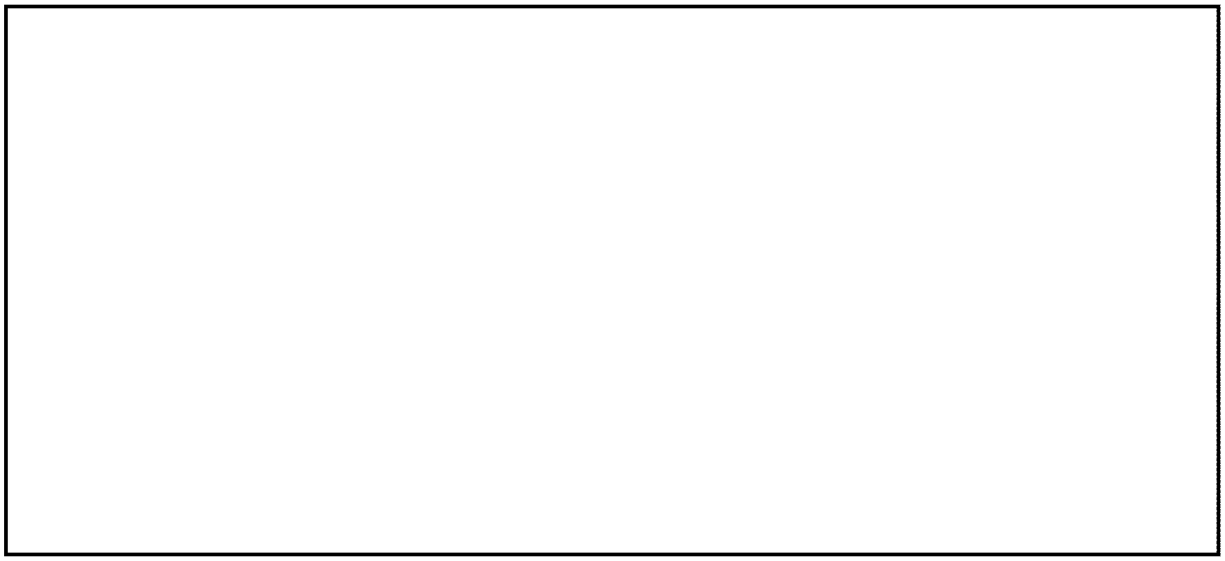
FISA currently defines "agent of a foreign power" to include a person who knowingly engages in clandestine intelligence gathering activities on behalf of a foreign power—but only if those activities "involve or may involve a violation of" federal criminal law. [redacted]

[redacted] b5

Section 103: Strengthening Wartime Authorities Under FISA.

Under 50 U.S.C. §§ 1811, 1829 & 1844, the Attorney General may authorize, without the prior approval of the FISA Court, electronic surveillance, physical searches, or the use of pen registers for a period of 15 days following a congressional declaration of war. [redacted]

[redacted] b5



b5

Title II: Protecting National Security Information

Section 201: Prohibition of Disclosure of Terrorism Investigation Detainee Information.

In certain instances, the release of information about persons detained in connection with terrorism investigations could have a substantial adverse impact on the United States' security interests, as well as the detainee's privacy. *Cf. North Jersey Media Group, Inc. v. Ashcroft*, 308 F.3d 198, 217-19 (3d Cir. 2002). Publicizing the fact that a particular alien has been detained could alert his coconspirators about the extent of the federal investigation and the imminence of their own detention, thus provoking them to flee to avoid detention and prosecution or to accelerate their terrorist plans before they can be disrupted.

b5

Section 202: Distribution of "Worst Case Scenario" Information.

Section 112(r) of the Clean Air Act, 42 U.S.C. § 7412(r), requires private companies that use potentially dangerous chemicals to submit to the Environmental Protection Agency a "worst case

scenario" report detailing what would be the impact on the surrounding community of release of the specified chemicals. Such reports are a roadmap for terrorists, who could use the information to plan attacks on the facilities.

b5

Section 203: Information Relating to Capitol Buildings.

The Congressional Accountability Act of 1995, 2 U.S.C. § 1301 et seq., establishes the Office of Compliance, a congressional office that has the power to enforce OSHA standards with OSHA often assists the

b5

Section 204: Ex Parte Authorizations Under Classified Information Procedures Act.

Under the current version of the Classified Information Procedures Act,18 U.S.C. App. 3 §§ 1-16, courts have discretion over whether to approve the government's request for a CIPA authorization—which enables the submission of sensitive evidence ex parte and in camera. See 18 U.S.C. App. 3 § 4 ("The court *may* permit the United States to make a request for such authorization [for a protective order] in the form of a written statement to be inspected by the court alone." (emphasis added)).

b5

[redacted] b5

Section 205: Exclusion of United States Security Requirements from Gross Income of Protected Officials.

Under current tax law, certain federal officials—those whose movements are restricted, or who are required to use specific facilities, for their physical protection in the interest of the United States' national security—may be taxed on the value of these protective "services." *See* 26 C.F.R. 1.132-5(m) (describing the circumstances under which police protection and related transportation expenses may be deemed to be working condition fringe benefits).

[redacted] b5

Section 206: Grand Jury Information in Terrorism Cases.

[redacted] b5

MEMORANDUM TO: [redacted] OLC b6 b7C

FROM: FBI-OGC /C. Steele

SUBJECT: Comments on 1-9-03 Draft of Domestic Security Enhancement Act

DATE: January 14, 2003

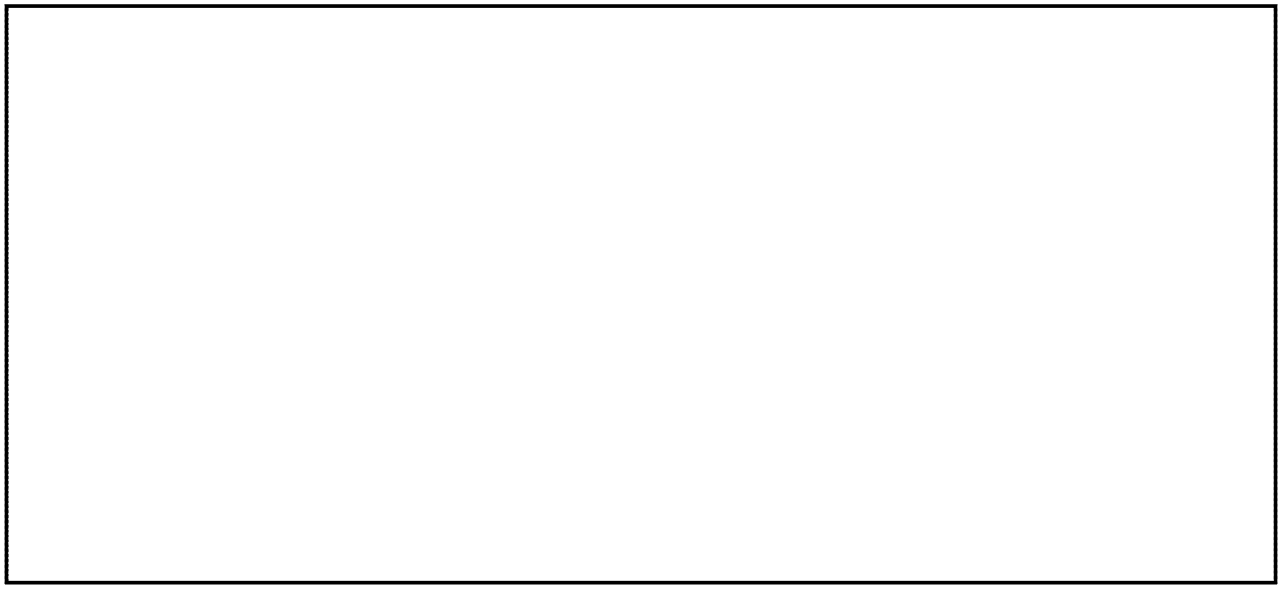
[redacted] b5

[redacted] b5

[redacted] b5

Additional Comments:

[redacted] b5



b5

b6
b7C

From: [redacted]
To:
Date: 1/14/03 10:06AM
Subject: Comments on statute

[redacted]

Here is a draft. Please feel free to make any edits. As you will see, I put in some language in support of [redacted] has seen this, but I am copying him. I am supposed to start a meeting at 10:15 that will take a while, so I am hoping that you can fax this to [redacted] (or I guess [redacted] can e-mail it). The fax number for [redacted]
Pat

b2
b6
b7C

CC: [redacted]

MEMORANDUM TO: [redacted] OLC b6 b7C

FROM: FBI-OGC

SUBJECT: Comments on 1-9-03 Draft of Domestic Security Enhancement Act

DATE: January 14, 2003

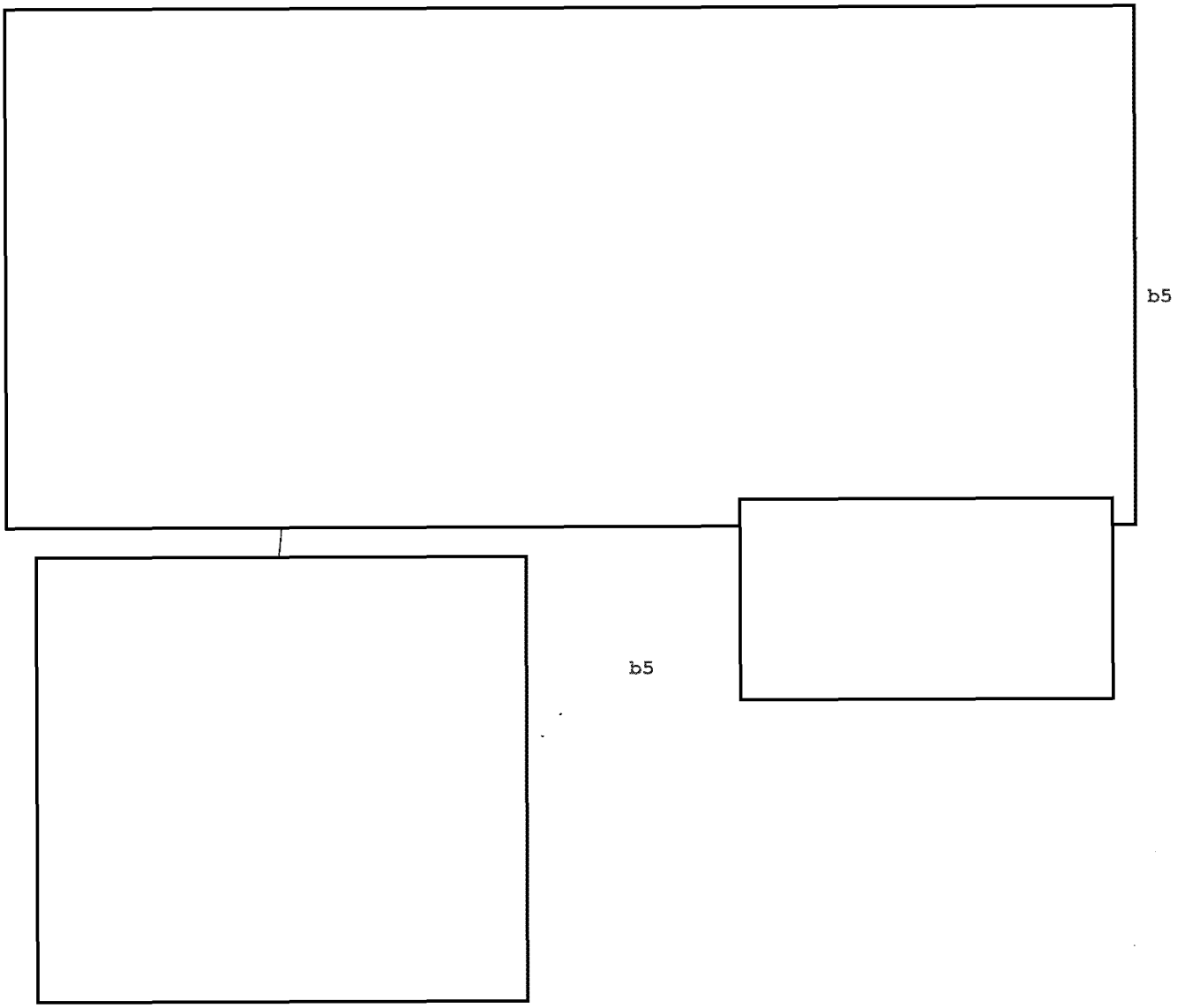
[redacted] b5

[redacted] b5

[redacted] b5

Additional Comments:

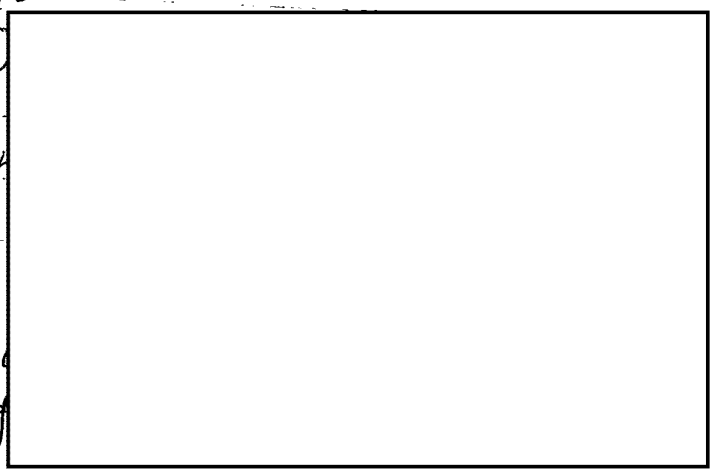
[redacted] b5


b5
b5

Spike's top 2 legislative issues:

(1)

(2)



b5

[redacted] b2 b7C

Section 102 = ~~Probable Cause~~

"reasonable belief" seems consistent w/ Gates "fair probability ~~that~~ the contention is true.

103 ~~test~~ = [redacted]

Section 108 ~~111~~ - [redacted]

[redacted] b5

126 [redacted]

128 -

Section 205 - [redacted]

Trying to get pre-Clearance -

Anticipate a new general circulation around the Dept.

109 - Enforcement / Ct Orders

Section 206 ~~206~~ Rule 6(e) secrecy requirement extends to witnesses

[redacted]

b5

Business Record NTL Sec Letters
Ca Credit Report NSL
Educational Records NSL
} But have admin Subpoena Power

NSL - Enforcement Mechanism
Not Sec Mail Covers

Tax Return Info

b6 b7C

From: [redacted]
To: Kelley, PATRICK; [redacted] b6
Date: 1/13/03 12:49PM b7C
Subject: Patriot 2

[redacted]ttached below are ALU's comments on OLP's 1/9 draft. (These are essentially the same as the comments we sent you on 1/8 re the 12/16 draft, and the e-mail observations below likewise apply to the 1/9 draft.) From ALU's perspective, the two drafts are essentially the same in not adopting (apart from a couple painfully narrow items) any of ALU's comments you sent to OLP on 11/15.

>>> PATRICK Kelley 01/10/03 08:54AM >>>
My quick review of the Jan. 2, edition fails to reflect any of ALU's suggested changes. May be that I missed them because the comments are keyed to the bill and I don't have a copy of the bill.

>>> PATRICK Kelley 01/10/03 08:37AM >>>
b6 [redacted] concur. However [redacted] gave me yesterday a Section-by Section Analysis dated Jan. 2nd. I didn't
b7C get the rest of the bill but I will send you what I have.

>[redacted]01/08/03 11:28AM >>>
[redacted] attached are our comments.

[redacted] b5

CC: Bowman, MARION; [redacted] Hardy, David; [redacted] b6
[redacted] b7C

Sensenbrenner Responses

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 147
Page 233 ~ Duplicate
Page 234 ~ Duplicate
Page 235 ~ Duplicate
Page 236 ~ Duplicate
Page 237 ~ Duplicate
Page 238 ~ Duplicate
Page 239 ~ Duplicate
Page 240 ~ Duplicate
Page 241 ~ Duplicate
Page 242 ~ Duplicate
Page 243 ~ Duplicate
Page 244 ~ Duplicate
Page 245 ~ Duplicate
Page 246 ~ Duplicate
Page 247 ~ Duplicate
Page 248 ~ Duplicate
Page 249 ~ Duplicate
Page 250 ~ Duplicate
Page 251 ~ Duplicate
Page 252 ~ Duplicate
Page 253 ~ Duplicate
Page 254 ~ Duplicate
Page 255 ~ Duplicate
Page 263 ~ Duplicate
Page 264 ~ Duplicate
Page 265 ~ Duplicate
Page 266 ~ Duplicate
Page 267 ~ Duplicate
Page 268 ~ Duplicate
Page 269 ~ Duplicate
Page 270 ~ Duplicate
Page 271 ~ Duplicate
Page 272 ~ Duplicate
Page 273 ~ Duplicate
Page 274 ~ Duplicate
Page 275 ~ Duplicate
Page 276 ~ Duplicate
Page 277 ~ Duplicate
Page 278 ~ Duplicate
Page 279 ~ Duplicate
Page 280 ~ Duplicate
Page 281 ~ Duplicate
Page 282 ~ Duplicate
Page 283 ~ Duplicate

Page 284 ~ Duplicate
Page 285 ~ Duplicate
Page 287 ~ Duplicate
Page 288 ~ Duplicate
Page 289 ~ Duplicate
Page 290 ~ Duplicate
Page 291 ~ Duplicate
Page 292 ~ Duplicate
Page 293 ~ Duplicate
Page 294 ~ Duplicate
Page 295 ~ Duplicate
Page 296 ~ Duplicate
Page 297 ~ Duplicate
Page 298 ~ Duplicate
Page 299 ~ Duplicate
Page 300 ~ Duplicate
Page 301 ~ Duplicate
Page 302 ~ Duplicate
Page 303 ~ Duplicate
Page 304 ~ Duplicate
Page 305 ~ Duplicate
Page 306 ~ Duplicate
Page 307 ~ Duplicate
Page 308 ~ Duplicate
Page 309 ~ Duplicate
Page 310 ~ Duplicate
Page 311 ~ Duplicate
Page 312 ~ Duplicate
Page 313 ~ Duplicate
Page 314 ~ Duplicate
Page 315 ~ Duplicate
Page 316 ~ Duplicate
Page 317 ~ Duplicate
Page 318 ~ Duplicate
Page 319 ~ Duplicate
Page 320 ~ Duplicate
Page 321 ~ Duplicate
Page 322 ~ Duplicate
Page 323 ~ Duplicate
Page 324 ~ Duplicate
Page 325 ~ Duplicate
Page 326 ~ Duplicate
Page 327 ~ Duplicate
Page 328 ~ Duplicate
Page 329 ~ Duplicate
Page 330 ~ Duplicate
Page 331 ~ Duplicate
Page 332 ~ Duplicate
Page 333 ~ Duplicate
Page 334 ~ Duplicate
Page 335 ~ Duplicate

Page 336 ~ Duplicate
Page 337 ~ Duplicate
Page 338 ~ Duplicate
Page 339 ~ Duplicate
Page 340 ~ Duplicate
Page 341 ~ Duplicate
Page 342 ~ Duplicate
Page 343 ~ Duplicate
Page 344 ~ Duplicate
Page 345 ~ Duplicate
Page 346 ~ Duplicate
Page 347 ~ Duplicate
Page 348 ~ Duplicate
Page 438 ~ Referral/Direct Dept of Justice
Page 439 ~ Referral/Direct DOJ
Page 440 ~ Referral/Direct DOJ
Page 441 ~ Referral/Direct DOJ
Page 442 ~ Referral/Direct DOJ
Page 443 ~ Referral/Direct DOJ
Page 444 ~ Referral/Direct DOJ
Page 445 ~ Referral/Direct DOJ
Page 446 ~ Referral/Direct DOJ
Page 447 ~ Referral/Direct DOJ
Page 448 ~ Referral/Direct DOJ
Page 456 ~ Referral/Direct DOJ
Page 457 ~ Referral/Direct DOJ
Page 458 ~ Referral/Direct DOJ
Page 459 ~ Referral/Direct DOJ
Page 460 ~ Referral/Direct DOJ
Page 461 ~ Referral/Direct DOJ
Page 462 ~ Referral/Direct DOJ
Page 463 ~ Referral/Direct DOJ
Page 464 ~ Referral/Direct DOJ
Page 465 ~ Referral/Direct DOJ
Page 466 ~ Referral/Direct DOJ
Page 467 ~ Referral/Direct DOJ
Page 468 ~ Referral/Direct DOJ
Page 469 ~ Referral/Direct DOJ
Page 470 ~ Referral/Direct DOJ
Page 471 ~ Referral/Direct DOJ
Page 472 ~ Referral/Direct DOJ
Page 473 ~ Referral/Direct DOJ
Page 474 ~ Referral/Direct DOJ
Page 475 ~ Referral/Direct DOJ
Page 476 ~ Referral/Direct DOJ
Page 477 ~ Referral/Direct DOJ
Page 478 ~ Referral/Direct DOJ
Page 479 ~ Referral/Direct DOJ
Page 480 ~ Referral/Direct DOJ
Page 481 ~ Referral/Direct DOJ
Page 482 ~ Referral/Direct DOJ

[redacted](OGC) (FBI)

From: [redacted](OGC) (FBI) b6 b7C
Sent: Monday, June 07, 2004 11:56 AM
To: [redacted](OGC) (FBI)
Subject: RE: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

UNCLASSIFIED
NON-RECORD

b6 b7C

It was [redacted] call, and I agree with him. [redacted] b1 b5

[redacted] (S)

[redacted] (S)

b6 b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, June 07, 2004 11:20 AM
To: [redacted](OGC) (FBI)
Subject: RE: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

b6 b7C

UNCLASSIFIED
NON-RECORD

Can I forward this to OCA? [redacted] b5

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, June 07, 2004 11:13 AM
To: [redacted](OGC) (FBI)
Subject: RE: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

b6 b7C

UNCLASSIFIED
NON-RECORD

b5 [redacted]

b6 [redacted]
b7C

-----Original Message-----
From [redacted](OGC) (FBI)
Sent: Monday, June 07, 2004 11:00 AM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted]
(OGC) (FBI); [redacted](OGC) (FBI)

b6
b7C

Cc: BOWMAN, MARION E. (OGC) (FBI)
Subject: FW: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act

~~UNCLASSIFIED~~
~~NON-RECORD~~

I know it is really short notice (I advised OCA that I did not think we could get our comments to them by 11:00 am) but if you have comments please let us know.
-----Original Message-----
From: [redacted] (OCA) (FBI)
Sent: Monday, June 07, 2004 9:06 AM
To: [redacted] OGC) (FBI); BOWMAN, MARION E. (OGC) (FBI) [redacted] (OGC) (FBI) [redacted] (CID) (FBI) [redacted] (CID) (FBI); [redacted] (CD) (FBI) [redacted] (CD) (FBI); [redacted] (CD) (FBI) [redacted] (CTD) (FBI) [redacted] (CTD) (FBI); [redacted] (DO) (FBI) [redacted] DO) (FBI) b6
Subject: Draft Response to Sen. Feinstein on Sunset Provisions of the USA Patriot Act b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

The attached testimony is being given before Congress. Please review the testimony and provide your comments, if any, to CAO. Please indicate if your division is in favor or opposed to the testimony as well as the reasons for your division's position. If your division opposes the testimony fully or in part, but believes that it can be remedied by changes in the verbiage, please describe in detail what should be added, deleted, or changed, including recommendations for substitute language sufficient to correct the objectionable section(s).

Please E-mail your comments to SSA [redacted] with a cc to [redacted] Your comments should be prepared in Microsoft Word format which is suitable for dissemination to DOJ and to congressional staff. Please send these comments to the CAO contact person as an attachment to your E-mail. If you have additional comments which are not suitable for dissemination, please include them in the body of your E-mail separate and apart from the attachment. If your division is not taking a position and has no comments, please send an E-mail to the CAO contact person stating such. b2 b6 b7C

DEADLINE 11:00 am 6-7-04. We appreciate your attention to this matter.

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

UNCLASSIFIED

UNCLASSIFIED

DATE: 12-07-2005
CLASSIFIED BY 65179 DMH/LP/DFW
REASON: 1.4 ((c) 06-CV-0845)
DECLASSIFY ON: 12-07-2030

[redacted] (OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Tuesday, May 18, 2004 3:08 PM
To: [redacted] (Div00) (FBI)
Cc: [redacted] (Div00) (FBI); [redacted] Div09) (FBI); [redacted] Div09) (FBI); BOWMAN, MARION E. (Div09) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

SECRET

b6 b7C
[redacted] please be advised that the use of 215 mentioned below just refers to a field office having submitted requests. As of last week, we still had not received a business record orde[redacted] (S) (S)
[redacted] We'll let you know no later than tomorrow what the response is.
b1
[redacted] (S)

-----Original Message-----
b6 **From:** [redacted] (Div09) (FBI)
b7C **Sent:** Tuesday, May 18, 2004 2:03 PM
To: [redacted] (Div00) (FBI); BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div00) (FBI)
Subject: RE: Statistics re USA PATRIOT Act provisions
b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] I can provide you the results from the field survey that OGC conducted, however, I can also guarantee that these are not entirely accurate numbers. The field survey was voluntary, and the level of detail provided varied between the field offices. Furthermore, since then I have been advised that some HQ divisions have been utilizing various Patriot Act tools, and I did not receive any contributions from any HQ division on this survey, so their use is not included in any numbers that I have.

The field offices reported the following:

Section 206 - Roving FISA orders [redacted] mes (S)
b1
Section 215 - Used [redacted] (S) additional orders currently in approval process (S)
Section 213 - Delayed Notice for Search Warrants - This is not a sunset provision, so we did not seek field input on this specific provision at this time.

Also - as you are aware, field offices collect statistics on their accomplishments (i.e. search warrants executed). I believe that Finance Division maintains, compiles, and reports these statistics. They may have more accurate field wide numbers.

I hope this is helpful.

[redacted]
b6
Assistant General Counsel
b7C

Investigative Law Unit
Office of the General Counsel
[redacted]

b6
b7C
b2

-----Original Message-----
From: [redacted] (Div00) (FBI)
Sent: Tuesday, May 18, 2004 1:41 PM
To: BOWMAN, MARION E. (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] (Div00) (FBI)
Subject: Statistics re USA PATRIOT Act provisions
Importance: High

~~UNCLASSIFIED~~
~~NON-RECORD~~

In anticipation of the Director's scheduled appearance before the Senate Judiciary Committee this Thursday, May 20th, we are trying to confirm the number of times we have used Delayed Notice (so-called "Sneak and Peek") Warrants, FISA Roving Wiretaps, and FISA Orders for Tangible Things (i.e., so-called Section 215 Orders), since passage of the USA PATRIOT Act.

I realize there are several potential complications with compiling such numbers (e.g., Delayed Notice Warrants used in traditional criminal cases, classification issues re 215 Orders, etc.). Nevertheless, if any of you could provide some input on this, it would be very helpful. We can almost guarantee the Director will be asked about the numbers when he testifies.

Is DOJ compiling numbers? Is there anyone at OLP or OIPR who may know?

Thanks,

[redacted]
Office of Congressional Affairs
ext. [redacted]

b2
b6
b7C

~~UNCLASSIFIED~~

UNCLASSIFIED

~~SECRET~~

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

DATE: 12-08-2005
CLASSIFIED BY 65179 DMH/LP/DFW
REASON: 1.4 ((C) 05-CV-0845)
DECLASSIFY ON: 12-08-2030

[redacted] OGC) (FBI)

From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 10:51 AM
To: [redacted] (Div00) (FBI)
Cc: [redacted] (Div09) (FBI); [redacted] (Div09) (FBI)
Subject: RE: Tools Question

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

I agree with what everyone has said. We have very limited admin subpoena powers, pe[redacted] email. Section 215 of the Patriot Act gave us a right to get business records [redacted] However, those records do require a FISA Court order. Admin subpoenas would be better because they do not require a court order. They are more like NSLs, which, as you probably know, are very restricted in scope inasmuch as we can only use them for communications providers, financial institutions, and credit reporting companies. If we simply want to get hotel records, for instance, we have no way of getting them now, and if we start using business records orders, we will have to go through the FISA court to get those. So that is why all this attention is focused on getting admin subpoenas - some way by which we do not have to go to court to get the information.

(S)

b1
b2
b7E

[redacted]

-----Original Message-----
From: [redacted] Div00) (FBI)
Sent: Friday, April 30, 2004 10:41 AM
To: [redacted] Div09) (FBI)
Cc: [redacted] (Div09) (FBI)
Subject: RE: Tools Question

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted] thanks - you're talking about §215 of the Patriot Act - right? I've attached [redacted] response fyi. If [redacted] has any other thoughts, feel free to share. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

-----Original Message-----
From: [redacted] (Div09) (FBI)
Sent: Friday, April 30, 2004 10:38 AM
To: [redacted] (Div09) (FBI); [redacted] (Div00) (FBI); [redacted] (Div09) (FBI)
Cc: [redacted] Div09) (FBI)
Subject: RE: Tools Question

b6
b7C

~~UNCLASSIFIED~~
~~NON-RECORD~~

[redacted]

I have a moment. b6 b7C

We have the right to collect business records under FISA which the PAtriot Act gave us. We have never used this authority.

[redacted]s the expert.

[redacted]

-----Original Message-----
From: [redacted](Div09) (FBI)
Sent: Friday, April 30, 2004 10:32 AM
To: [redacted](Div00) (FBI); [redacted](Div09) (FBI); [redacted](Div09) (FBI)
b6 b7C
Subject: RE: Tools Question

~~UNCLASSIFIED~~
NON-RECORD

[redacted] The FBI has no comparable authority that I know of--and I am not surprised because that summons provision is strictly under Treasury's regulatory function. As I read the statute, the information provided cannot be used for criminal investigative purposes. That same section goes on to establish authority for Suspicious Activity Reports, which the banks are required to file and which are the primary means by which they notify Treasury of potential criminal transactions--which can then be shared with FBI. FBI's admin aubpoena authority is limted to 3 areas--drugs under 21 USC 876 and child pornography and health care fraud under 18 USC 3486.

[redacted]

-----Original Message-----
From: [redacted](Div00) (FBI)
Sent: Thursday, April 29, 2004 6:08 PM
b6 b7C
To: [redacted](Div09) (FBI); [redacted](Div09) (FBI); [redacted]
(Div09) (FBI)
Subject: Tools Question

~~UNCLASSIFIED~~
NON-RECORD

We got the following question from our friends on the House Judiciary Committee who have been looking at NSLs and admin subpoena issues - 31 USC 5318(a)(4) gives the Secretary of the Treasury administrative subpoena authority to obtain business records in specific cases. Does the FBI have any comparable authority? I'd appreciate any assistance you could provide. Thanks,

[redacted] b6 b7C
Office of Congressional Affairs

[redacted] b2

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SECRET

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 2
Page 6 ~ Duplicate
Page 7 ~ Duplicate

SSCI Briefing - 4/2005

b6
b7C

SECRET

Copy

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

Valerie E. Caproni
SSCI Briefing
USA PATRIOT Act Renewal
April 2005

(This cover sheet is unclassified.)

SECRET

704-101
NSN 7540-01-213-7902

STANDARD FORM 704 (8-85)
Prescribed by GSA/ISOO
32 CFR 2003

USA PATRIOT Act
Reauthorization Hearing
Valerie E. Caproni
FBI General Counsel
Senate Select Committee on Intelligence

TABLE OF CONTENTS

The "Wall", the USA PATRIOT Act and the Evolution of FBI International Terrorism Investigations Since 9/11

(U) A major benefit of the USA PATRIOT Act ("the Act"), as it pertains to the so-called "Wall" that existed prior to 9/11 between the law enforcement and intelligence communities, has to do with speed and efficiency. There are specific provisions in the Act that authorized the sharing of intelligence information gathered via criminal investigative techniques with the intelligence community. These include Section 203, which, for example, allowed federal grand jury and wiretap information to be shared with the intelligence community. The sections of the Act having to do with the activities of the intelligence community were geared towards harmonizing the law to fit contemporary technological realities. They were also meant to ease somewhat the thresholds required to obtain certain types of information in intelligence investigations. The broad effect of the Act was thus to foster an environment in which information could flow between the two communities robustly and sensibly. Law enforcement and intelligence personnel are now able to work together at the earliest possible stages in order to combat international terrorism. Nothing can replace the raw investigative effort exerted by criminal and intelligence investigators. But the PATRIOT Act has enabled these investigators to do their jobs more quickly, with fewer barriers and with more ability to integrate information.

(U) ~~(S)~~ Once the PATRIOT Act had been passed in October 2001, information began to flow more readily between law enforcement and the intelligence community. One of the more crucial examples of this movement was the sharing of information between the national security side of the FBI and the DOJ Criminal Divisions and U.S. Attorneys. In March 2002, the Attorney General issued intelligence sharing procedures mandating that FBI counterterrorism officials would be required to provide international terrorism case file information with criminal prosecutors. This sharing initially began as a review of files and later evolved into a close working relationship between the FBI Counterterrorism Division (CTD) and the DOJ Criminal Division's Counterterrorism Section (CTS). CTS, moreover, helps to act as a bridge between the FBI and the United States Attorneys throughout the country.

(U) ~~(S)~~ Later, in July 2002, the Foreign Intelligence Surveillance Court (FISC) added a new component to the spectrum of intelligence sharing. Up to that time, the minimization procedures adopted pursuant to the Foreign Intelligence Surveillance Act (FISA) did not allow for the dissemination – from FBI to CIA or NSA -- of international terrorism foreign intelligence data that had been collected under FISA authority to be shared in its so-called "raw" form. In other words, the FBI would have to have first minimized the data before sharing it with the CIA or the NSA. The FISC changed this by allowing NSA and CIA to have access to the data. Those agencies thus could greatly speed up the process of bringing their resources to bear in working on the common transnational terrorism threats we now face. Moreover, because the PATRIOT Act had brought the criminal investigators closer to the intelligence community through the FBI, by mid-2002 there began to emerge true integration among several of the agencies engaged in this effort.

(U)

(S) In August 2002, the Attorney General enhanced intelligence sharing with international partners. The AG issued procedures allowing the CIA and NSA to disseminate FISA-derived foreign intelligence relating to United States Persons (USPERs) to foreign governments without having to return to the AG for authorization in each discrete instance. The Attorney General instead required that, while the CIA and NSA could disseminate the information on an ongoing basis, they had to report the disseminations to him in a report on at least an annual basis. Thus, the same protections could be kept while ensuring that vital information moved to our international partners quickly.

(U) In September 2002, the Attorney General issued guidelines regarding the movement of intelligence information from criminal investigations and proceedings into the intelligence community. These guidelines focused on Sections 203 and 905 of the PATRIOT Act. Intelligence acquired during the course of criminal investigations is mandated by Section 905 to be disclosed to the Director of Central Intelligence and Homeland Security officials. Section 203 more specifically authorizes grand jury, electronic, wire and oral interception information to be shared with the intelligence community.

(U) Overall, the PATRIOT Act made a number of specific changes that directly benefited the FBI in its investigations. Section 505 allowed National Security Letters (NSLs) to be issued under a relevance standard. This requires the FBI to demonstrate that the request is relevant to on ongoing national security investigation. Section 206 gave the FBI roving wiretap authority under FISA. The roving provision operates like roving authority under criminal law statutes. Section 207 increased the duration of FISA coverage to permit FBI field offices to monitor FISAs for longer periods. All agents of a foreign power searches increased from 45 to 90 days and for Non-U.S. Person officers or employees of foreign powers the initial FISA period of coverage increased to 120 days. Renewals on such applications were extended to one year of coverage. Section 203 (mentioned above) has allowed intelligence gathered through certain criminal process to be shared with the intelligence community. Section 214 changed the FISA Pen Register/Trap and Trace standard to relevance. This has allowed for robust use of the Pen Register/Trap and Traces in the initial stages of national security investigations and has helped the FBI to build a better picture of connections among suspected international terrorist subjects. Finally, Section 208 modified the FISA statute by increasing the number of judges on the court. This has eased the burden on all involved in the FISA process. Moreover, three FISA judges are now located within fifty miles of Washington, DC. All of the above tools have greatly enabled the FBI to ensure that the law enforcement and intelligence communities have the ability to share information in the effort to confront international terrorism.

(U) In November 2002, the last vestiges of the "Wall" disintegrated when the Foreign Intelligence Surveillance Court of Review issued its very first opinion. In that opinion, the court affirmed the March 2002 Attorney General intelligence information sharing procedures (the FISC had limited them somewhat in May 2002). Further, the Foreign Intelligence Surveillance Court of Review opinion had the effect of declaring the

"Wall" to have been a misinterpretation of the FISA statute and other guidance. The court stated that under the FISA statute as originally written, the government needed to show that only "a purpose" for the collection or search was to gather foreign intelligence rather than the "sole purpose." The court noted that the PATRIOT Act modified the standard to a "significant purpose." The overall effect of the opinion was to bolster the push behind the PATRIOT Act to integrate law enforcement and intelligence efforts, within clear guidance, and to banish misperceptions about the "Wall."

(U) In January 2003, the President announced the creation of the Terrorist Threat Integration Center (TTIC) in his State of the Union Address. TTIC and its successor, the National Counterterrorism Center (NCTC)(created by executive order in August 2004 and affirmed by statute in December 2004), have been responsible for integrating all terrorism analytical threat reporting in a single entity. All intelligence community databases are accessible at NCTC. Intelligence information gleaned from criminal proceedings, such as federal grand juries, is disseminated to NCTC and is integrated into national intelligence reporting. Section 203 of the PATRIOT Act has allowed this to happen.

(U) ~~(S)~~ In October 2003, the Attorney General issued revised Guidelines for National Security Investigations and Foreign Intelligence Collection (NSIG). These guidelines reflect the evolution of changes in national security law, intelligence collection and international terrorism investigations that occurred over the preceding two years. The NSIG reflect the integrated nature of national security investigations and recognize the need to use all available investigative tools, both criminal and intelligence, to combat current transnational threats. The NSIG themselves are a powerful statement on new realities, ones that reflect the need for information integration between criminal investigations and intelligence investigations.

(U) In the year and a half since the creation of the NSIG, the 9/11 Commission has issues its reports and recommendations, and the President signed intelligence reform legislation. The FBI continues to evolve, working towards building a strong Directorate of Intelligence while continuing its law enforcement mission. As the integrated approach to battling International Terrorism evolves, the FBI continues to rely on the provisions of the PATRIOT Act. The Act has enabled the FBI to obtain important information more efficiently than before, allowing its investigators to focus more effectively on their cases. The Act is one of the underpinnings of bringing law enforcement and intelligence services together. If the Congress were to allow the Sunset provisions to lapse, it would be depriving the intelligence and law enforcement communities of valuable and necessary tools. It also would send a signal at odds with the evolution in national security investigations over the last three and half years. The intelligence community has been told repeatedly to "connect the dots" since 9/11. With the help of the law enforcement community, it has made progress. The 9/11 Commission has embraced the value of the PATRIOT Act. The FBI asks that Congress reinforce these views.

Post 9/11 Timeline on Measures to Increase Information Sharing and Create Fully Integrated International Terrorism Investigations

1. September 11, 2001

- (U) Terrorist attacks.

2. October 2001

- (U) Passage of the USA PATRIOT Act.
  - Makes technical changes to standards for securing NSLs, Business Records, Voicemail Communications, Computer Trespassing, etc.
  - Abolished the "Wall" for the sharing of Title III and Federal Grand Jury Rule 6(e) material with the U.S. Intelligence Community.

3. March 2002

- (U) Attorney General issues Intelligence Sharing Procedures for Foreign Intelligence and Counterintelligence Investigations. Procedures mandate that Federal Prosecutors will review FBI International Terrorism case files for relevant material on which to build criminal prosecutions.

4. May 2002

- (U) FISC accepts in part and modifies in part the AG March 2002 procedures. Creates a "chaperone" requirement instituting OIPR involvement in information sharing between intelligence investigators and criminal prosecutors.

5. July 2002

(U)
- ~~(S~~//NF) FISC approves the "Raw Data" Motion and signs order. This order permits the FBI to share raw FISA data with the CIA and NSA in International Terrorism FISA surveillances and searches.

6. August 2002

(U)
- ~~(S~~//NF) Attorney General signs standing authorization for CIA and NSA to disseminate USPER FISA-derived foreign intelligence to foreign governments. This authorization allows the CIA and NSA to disseminate the material without having to seek AG approval in each discrete instance.

7. September 2002

- (U) Attorney General issues "Guidelines Regarding the Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation." Explains implementation of PATRIOT Act Section 905(a).

- (U) Attorney General issues "Guidelines Regarding Prompt Handling of Reports of Criminal Activity Involving Foreign Intelligence Sources." Explains implementation of PATRIOT Act Section 905(b).

- (U) Attorney General issues "Guidelines for Disclosure of Grand Jury and Electronic, Wire and Oral Interception Information Identifying United States Persons." Explains implementation of PATRIOT Act Section 203.

8. November 2002

- (U) FISA Court of Review issues opinion rejecting the OIPR "chaperone" requirement and accepts AG March 2002 Information Sharing in full. FISA Court of Review also states that FISC and DOJ have incorrectly interpreted the FISA statute for years. FISA Court of Review opinion has effect of declaring the "Wall" to have been a misinterpretation of the statute and other guidance. The FISA Court of Review states that under the FISA statute as originally written the government needed to show that "a purpose" for the collection was to gather Foreign Intelligence rather than the "sole purpose." The FISA Court of Review notes that the PATRIOT Act modified the standard to a "significant purpose."

9. December 2002

- (U) The Deputy Attorney General (DAG) issues field guidance to all DOJ prosecutors and all FBI agents on Intelligence Sharing in FI and FCI Investigations. The DAG also explains the effect of the FISA Court of Review opinion.

10. January 2003

- (U) The Creation of the Terrorist Threat Integration Center ("TTIC") (now the National Counterterrorism Center) announced by the President.

11. March 2003

- (U) Department of Homeland Security is created.

12. October 2003

- (U) Attorney General issues revised Guidelines for National Security Investigations and Foreign Intelligence Collection. ("NSIG")

[redacted]

4/19/05
1:15 PM

THESE ARE ALL THE SUPPLEMENTAL MATERIALS FOR THE SSCI PATRIOT ACT BOOK.

b6
b7C

[redacted]

Cases Using FISA (Public Information)
Prepared by the Department of Justice Counterterrorism Section

United States v. Al-Arian, et al.

- **Defendants:** Sami Amin Al-Arian, Ramadan Abdullah Shallah, Bashir Musa Mohammed Nafi, Sameeh Hammoudeh, Mohammed Tasir Hassan Al-Khatib, Abd Al Aziz Awda, Ghassan Zayed Ballut, Hatim Naji Fariz, Mazen Al-Najjar
- **District:** Middle District of Florida, Judge James Moody
- **Date of Superceding Indictment:** September 21, 2004
- **Status:** Trial scheduled to begin May 16, 2005.

United States v. Arnaout

- **Defendant:** Enaam M. Arnaout
- **District:** Northern District of Illinois, Judge Suzanne B. Conlon
- **Date of Indictment:** October 9, 2002
- **Status:** Arnaout ultimately pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

United States v. Hassoun, Youssef

- **Defendants:** Adham Hassoun and Mohamed Youssef
- **District:** Southern District of Florida; Judge Marcia Cooke
- **Date of Third Superceding Indictment:** October 7, 2004
- **Status:** Awaiting trial.

United States v. Holy Land Foundation for Relief & Development, et al.

- **Defendants:** Shukri Abu Baker, Mohammed El-Mezain, Ghassan Elashi, Haitham Maghawri, Akrim Mishal, Mufid Abdulqader, and Abdulraham Odeh
- **District:** Northern District of Texas, Judge Joseph A. Fish
- **Date of Indictment:** July 26, 2004

- **Status:** The defendants have been indicted, still waiting for a trial date to be set.

United States v. Damrah

- **Defendants:** Fawaz Mohammed Damrah
- **District:** Northern District of Ohio, Judge James Gwin
- **Date of Indictment:** December 16, 2003
- **Status:** On June 17, 2004, the jury convicted Fawaz Damrah of violating 18 U.S.C. § 1425 by unlawfully obtaining U.S. citizenship by concealing material facts. On September 20, 2004, the defendant was committed to the Bureau of Prisons for two months, followed by four months in home confinement with electronic monitoring, and three years of supervised release. On September 23, the district court ordered the defendant's citizenship revoked pursuant to 8 U.S.C. § 1451(e).

United States v. Battle, et al. **(Portland Cell)**

- **Defendants:** Jeffrey Leon Battle, October Martinique Lewis, Patrice Lumumba Ford, Muhammad Ibrahim Bilal, Ahmed Ibrahim Bilal, Habis Abdulla al-Saoub, Maher Mofeid Hawash
- **District:** District of Oregon, Judge Robert E. Jones
- **Date of Superceding Indictment:** May 2, 2003
- **Status:** Six of the seven were convicted and received prison sentences ranging from three to eighteen years. Charges against the seventh defendant (al-Saoub) were dismissed after he was killed in Pakistan by Pakistani troops on October 3, 2003.

United States v. Dumeisi

- **Defendant:** Khaled Abdel Latif Dumeisi
- **District:** Northern District of Illinois
- **Date of Superceding Indictment:** October 29, 2003 (PACER)
- **Status:** Sections 218 and 504 were critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq, as well as two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United

Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible violations of criminal law. Because of this coordination, law enforcement agents and prosecutors learned from intelligence officers of an incriminating telephone conversation that took place in April 2003 between Dumeisi and a co-conspirator. This phone conversation corroborated other evidence that Dumeisi was acting as an agent of the Iraqi government and provided a compelling piece of evidence at Dumeisi's trial. (Excerpt from *The Report from the Field* (July 2004))

Cases Using FISA (Public Information)
Prepared by the Department of Justice Counterterrorism Section

United States v. Al-Arian, et al.

- **Defendants:** Sami Amin Al-Arian, Ramadan Abdullah Shallah, Bashir Musa Mohammed Nafi, Sameeh Hammoudeh, Mohammed Tasir Hassan Al-Khatib, Abd Al Aziz Awda, Ghassan Zayed Ballut, Hatim Naji Fariz, Mazen Al-Najjar
- **District:** Middle District of Florida, Judge James Moody
- **Status:** Trial scheduled to begin May 16, 2005.

United States v. Arnaout

- **Defendant:** Enaam M. Arnaout
- **District:** Northern District of Illinois, Judge Suzanne B. Conlon
- **Status:** Arnaout ultimately pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

United States v. Hassoun, Youssef

- **Defendants:** Adham Hassoun and Mohamed Youssef
- **District:** Southern District of Florida; Judge Marcia Cooke
- **Status:** Awaiting trial.

United States v. Holy Land Foundation for Relief & Development, et al.

- **Defendants:** Shukri Abu Baker, Mohammed El-Mezain, Ghassan Elashi, Haitham Maghawri, Akrim Mishal, Mufid Abdulqader, and Abdulraham Odeh
- **District:** Northern District of Texas, Judge Joseph A. Fish
- **Status:** The defendants have been indicted, still waiting for a trial date to be set.

United States v. Damrah

- **Defendants:** Fawaz Mohammed Damrah
- **District:** Northern District of Ohio, Judge James Gwin

- **Status:** On June 17, 2004, the jury convicted Fawaz Damrah of violating 18 U.S.C. § 1425 by unlawfully obtaining U.S. citizenship by concealing material facts. On September 20, 2004, the defendant was committed to the Bureau of Prisons for two months, followed by four months in home confinement with electronic monitoring, and three years of supervised release. On September 23, the district court ordered the defendant's citizenship revoked pursuant to 8 U.S.C. § 1451(e).

***United States v. Battle, et al.* (Portland Cell)**

- **Defendants:** Jeffrey Leon Battle, October Martinique Lewis, Patrice Lumumba Ford, Muhammad Ibrahim Bilal, Ahmed Ibrahim Bilal, Habis Abdulla al-Saoub, Maher Mofeid Hawash

- **District:** District of Oregon, Judge Robert E. Jones

- **Status:** Six of the seven were convicted and received prison sentences ranging from three to eighteen years. Charges against the seventh defendant (al-Saoub) were dismissed after he was killed in Pakistan by Pakistani troops on October 3, 2003.

United States v. Dumeisi

- **Defendant:** Khaled Abdel Latif Dumeisi

- **District:** Northern District of Illinois

- **Status:** Sections 218 and 504 were critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq, as well as two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible violations of criminal law. Because of this coordination, law enforcement agents and prosecutors learned from intelligence officers of an incriminating telephone conversation that took place in April 2003 between Dumeisi and a co-conspirator. This phone conversation corroborated other evidence that Dumeisi was acting as an agent of the Iraqi government and provided a compelling piece of evidence at Dumeisi's trial. (Excerpt from *The Report from the Field* (July 2004))

United States v. Hassoun and Youssef: On **September 16, 2004**, ADHAM HASSOUN and MOHAMMED YOUSSEF, were indicted by a Grand Jury in the Southern District of Florida in a **10-count superseding** indictment. The charges include: Providing material support to terrorists in violation of 18 USC § 2339A and also conspiracy to do the same for providing "material support and resources... knowing and intending that they be used in preparation for and carrying out a violation of Title 18 USC § 956 (a)(1), that is, a conspiracy to murder, kidnap and maim persons in a foreign country." The indictment also includes eight additional counts against HASSOUN on charges of unlawful possession of a firearm, making false statements, perjury and obstruction of immigration court proceedings. HASSOUN is currently in custody on these charges. YOUSSEF is in custody in Egypt serving a sentence for other terrorist activities. On **October 7, 2004**, the Grand Jury returned a superceding indictment against HASSOUN and YOUSSEF which charges them with, in addition to the earlier charges, one count each of conspiracy to murder, maim and kidnap persons in a foreign country in violation of 18 USC Section 956.

United States v. Arnaout: Enaam Arnaout, aka Abu Mahmoud Al Suri, aka Abu Mahmoud Al Hamawi, aka Abdel Samia, the **principle officer of the Benevolence International Foundation (BIF)**, was indicted by a Federal grand jury seated in the Northern District of Illinois. Arnaout was charged in an **eight (8) count indictment** with violating Federal criminal statutes to include **RICO (racketeering)**, conspiracy to provide material support to terrorism, mail fraud, wire fraud, and money laundering. On February 10, 2003, entered into a plea agreement with the government, pleading guilty to a RICO count. In August 2003, Arnaout was sentenced to serve an eleven (11) year prison sentenced related to the above RICO charges.

United States v. Dumeisi: January 12, 2004, KHALED ABDEL-LATIF DUMEISI was convicted in U.S. District Court, Northern District of Illinois in docket # 03-664, of acting as an unregistered agent of the former Government of Iraq (GOI). This conviction was the culmination of a long running FBI investigation into his activities on behalf of the GOI. The jury also found DUMEISI guilty of conspiracy and perjury. On March 31, 2004, he was sentenced to 46 months in prison, after which he will be deported.

United States v. Battle: On 03 October 2002, a federal grand jury in Portland, Oregon, indicted Jeffrey Leon Battle and five others for: Conspiracy to Levy War Against the United States (18 U.S.C. § 2384); Conspiracy to Provide Material Support & Resources to Foreign Terrorist Organizations (18 U.S.C. § 2339B); Conspiracy to Contribute Services to al Qaeda and Taliban (50 U.S.C. § 1705(b)). In addition, Battle and 3 others were indicted for Possessing Firearms in Furtherance of Crimes of Violence (18 U.S.C. §924(c)(1)(A)(iii)). Battle pled guilty to the first count of the indictment and was sentenced to 18 years incarceration on 24 November 2003. Other defendants received sentences from 3 - 18 years incarceration. Charges against one defendant were dismissed.

~~SECRET~~
RECORD 315 Q

United States v. Damrah

b6
b7C

On **December 16, 2003,** an indictment was handed down in the Nothern District of Ohio against Damrah for violation of Title 18 USC §§1425(a)(b), Imigration fraud charges. He was charged and found guilty of making false statements in connection with his citizenship application. He was convicted last year of lying to immigration authorities. He did not disclose during naturalization proceedings in 1993 that he helped raise money for PIJ. Damrah was sentenced to Jail for two months around the 21st of November (released end of January, 2005). After two months in prison, he spent another four months under house arrest. The Judge in the case was assured by the Prosecutor's office that no deportation proceedings were to be initiated until after DAMRAH had exhausted **all** appeals on the conviction. Damrah is currently facing deportation proceedings after being stripped of his US citizenship.

United States v. Holy Land Foundation for Relief & Development, et al.

On Monday, **07/26/2004,** sealed indictments and arrest warrants were obtained on charges of Conspiracy, Material Support to Terrorism, Money Laundering, and Tax fraud, in the Northern District of Texas.

The Holy Land Foundation for Relief and Development (HLFRD) is registered as a non-profit humanitarian organization that has conducted fund-raising activities in the United States and has claimed to provide aid to thousands of poor Palestinians in Gaza and the West Bank, as well as other geographical areas. On 12/04/2001, the Department of Treasury's Office of Foreign Assets Control (OFAC) designated the HLFRD as a Specially Designated Terrorist (SDT), and blocked all known assets of the HLFRD based on information that the HLF provided material support to the Foreign Terrorist Organization (FTO)/SDT HAMAS. On 12/10/2001, Dallas opened a criminal investigation into the HLFRD for providing material support to terrorism. Investigation has revealed that the targeted subjects provided material support to Hamas, and that they have committed various other violations of US law.

United States v. Al Arian, et al.

Superseding Indictment on September 21, 2004

Tampa FBI has been involved in a long-term criminal investigation of the North American cell of the PIJ terrorist organization. The cell is headed by Sami Al-Arian, a college professor, who operated numerous front organizations, namely the Islamic Committee for Palestine (ICP) and the World and Islam Studies Enterprises (WISE). These organizations not only raised funds to send back to the Middle East, but also employed Ramadan Shallah in Tampa, Florida, immediately before Shallah took over the leadership of the PIJ in1996 following the assassination of Fathi Shikaki.

The case is being prosecuted under a RICO theory. The indictment of Al-Arian and seven others took place on **February 19, 2003**. Sami Al-Arian, Sameeh Hammoudeh, Hatim Naji Fariz, and Ghassan Ballout were arrested on **February 20, 2003**. A superceding indictment was filed on the case on **September 21, 2004**, which added additional charges and overt acts, streamlined the prosecutive theory, and added subject Mazen Al-Najjar, who was previously named as an unindicted co-conspirator. The theory of the case is that PIJ is a criminal enterprise which uses various officers to conduct its illegal business through a pattern of racketeering activity in violation of 18 USC §§1962. The subjects of the investigation, acting through PIJ, have facilitated the murder of U.S. and Israeli citizens, have committed bombings and other criminal acts, and have then released public statements claiming responsibility for those criminal acts as a means to extort political concessions from the State of Israel in violation of 18 USC §§1961. The subjects have also financially supported PIJ and its campaign of terror by raising funds in the U.S. and Europe. Those funds were then forwarded from the Tampa, Florida area, to the Middle East to assist PIJ in carrying out specified unlawful activities (murder, extortion, destruction of property by explosion, etc.) in violation of the Money Laundering statute, 18 UCS §§1956. The subjects have also provided material support for terrorist activities in violation of 18 USC §§2339A and have aided and abetted the murder of U.S. citizens, namely Alissa Flatow and others, in violation of 18 UCS §§2332.

~~DERIVED FROM: Multiple Sources~~
~~DECLASSIFY ON: 20150418~~
~~SECRET~~

~~SECRET//ORCON,NOFORN~~

(S)

DATE: 08-18-2005
CLASSIFIED BY 65179 DMH/KBR
REASON: 1.4 ((C))
DECLASSIFY ON: 08-18-2030

b1 , b2, b6, b7C, b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S) b1 , b2, b6, b7C, b7E

box 3 last row classified per OGA letter dated 8/10/05

box 3 on line one classified per OGA letter dated 8/10/05

(S)

b1 , b2, b6, b7C, b7E

b1 , b2, b6, b7C, b7E

(S)

b1 , b2, b6, b7C, b7E

(S)

b1 , b2, b6, b7C, b7E

(S)

b1 , b2, b6, b7C, b7E

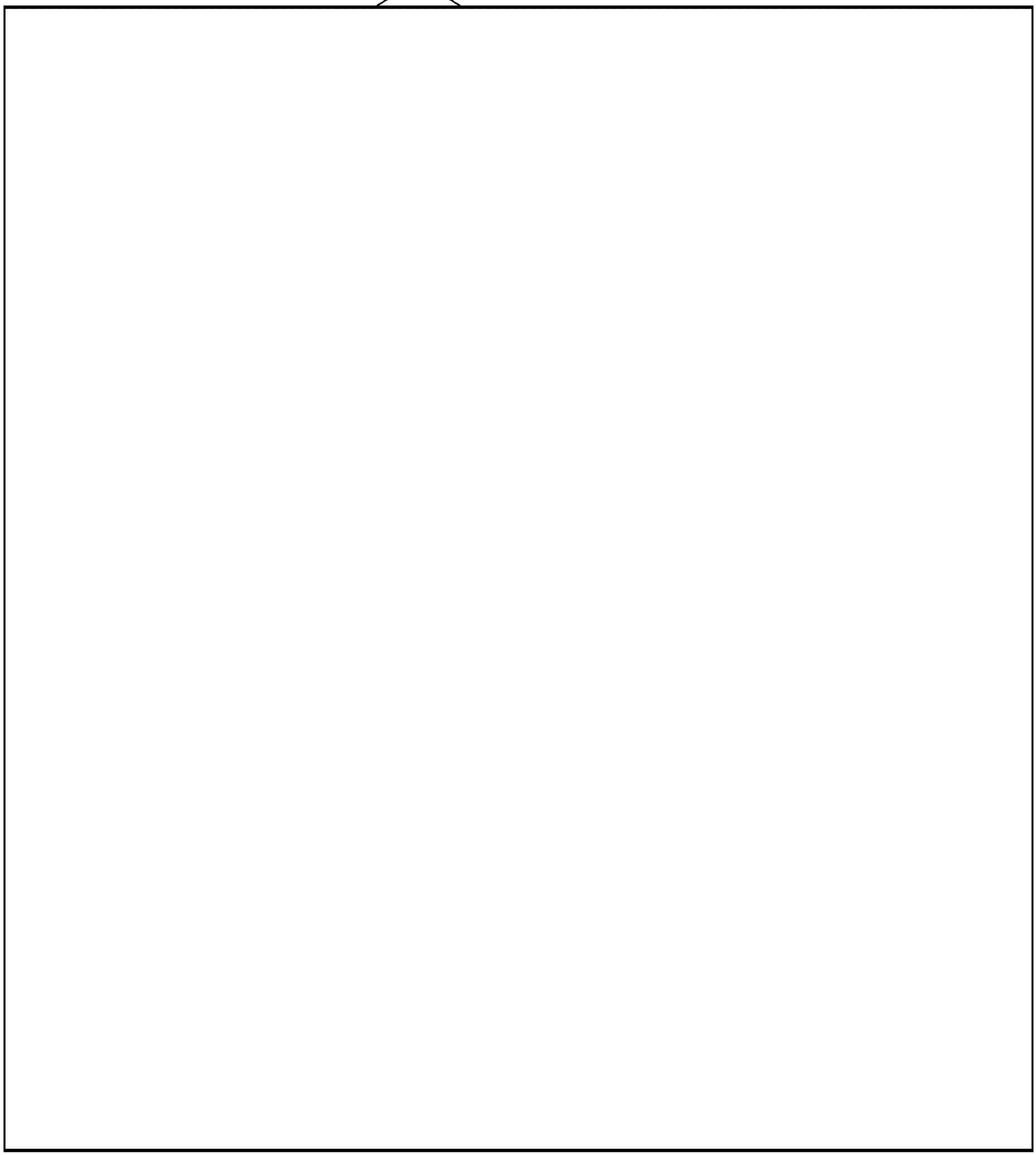
(S)

b1 , b2, b6, b7C, b7E

(S)

b1 , b2, b6, b7C, b7E

(S)



(S)

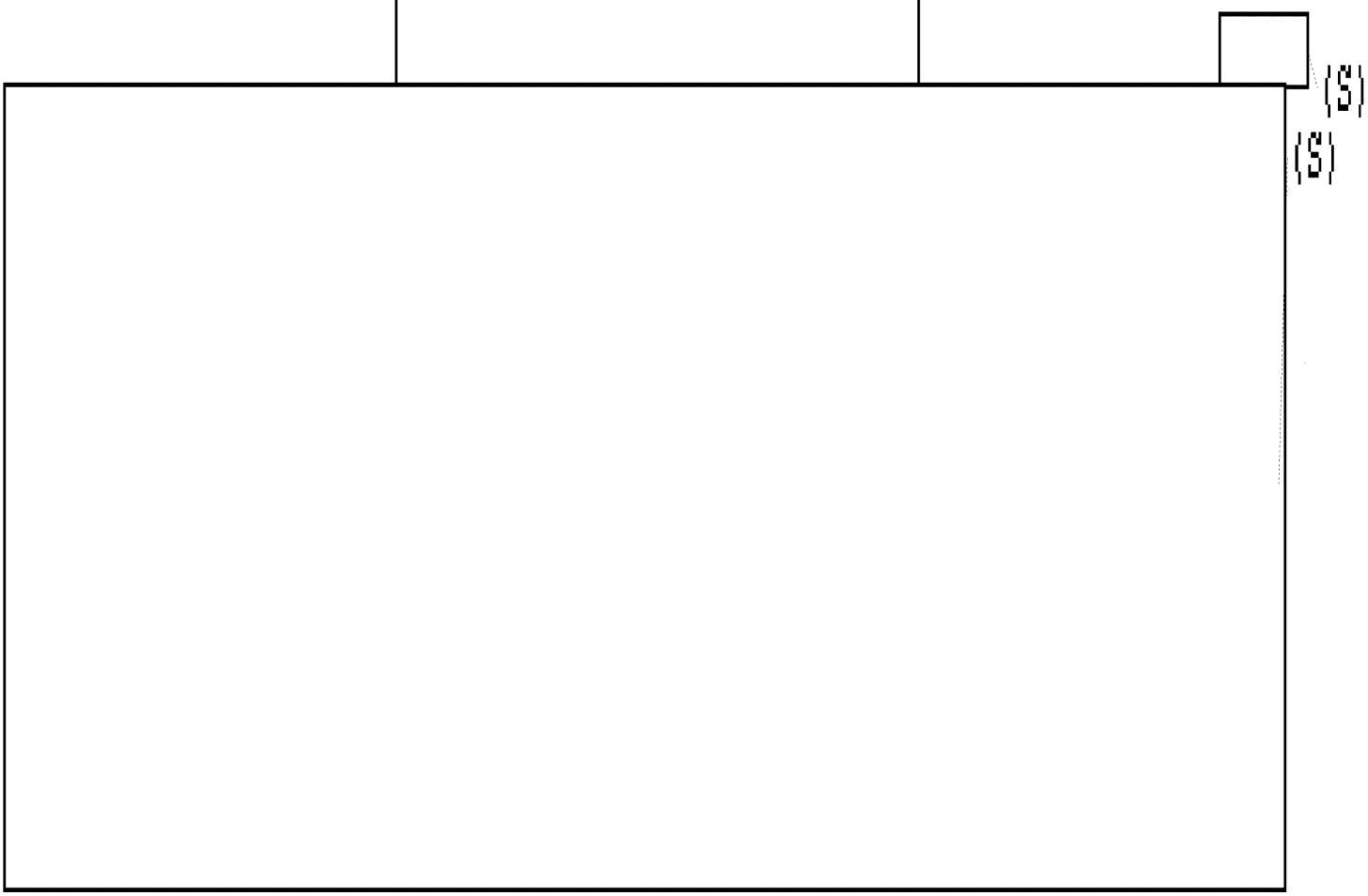
(S)

General Comments from SSA , CONUS 1, who did the first and has done the most

b2
b6
b7C
b7E

b1 , b2, b7E

b1 , b2, b7E



(S)

(S)

Name/Foreign Power: (S) b1 b6 b7C

b6 , b7C

Declarant: SSA

Docket No. & Date Approved: (S) b1

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

Background Facts:

b6
b7C

~~(S)~~ (U)

Reason For Initial Application:

(S) b1 b2 b6 b7C b7E

b1
b2
b6
b7C
b7E

Facts For Renewals:

(S)

~~(S)~~ (U)

(S) b1 b2 b6 b7C b7E

(U)

Name/Foreign Power: [redacted] (S)

Declarant: SSA [redacted]

Docket No. & Date Approved: [redacted] (S)

Background Facts:

(U) (S) [redacted]

(U) (S) [redacted]

(S) [redacted] (S)

(U) (S) [redacted] (S) (S)

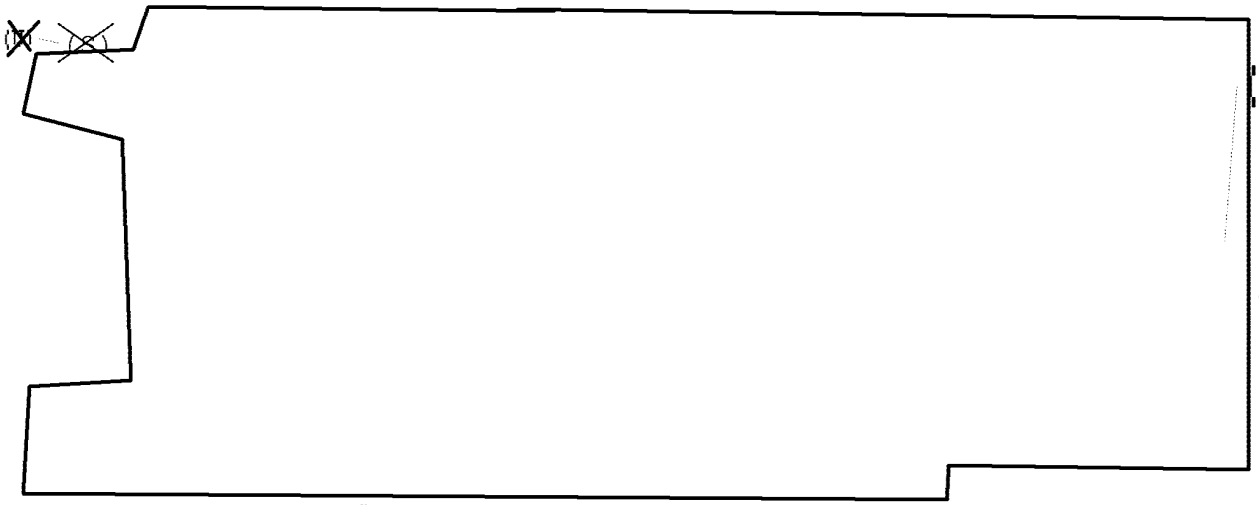
(S)

Reason For Initial Application:

(S) [redacted] (S)

(S) [redacted] (S)

~~SECRET~~



Facts For Renewals:

No Renewals.

Benefit (or lack thereof) of Roving Authority:

None cited in application; No information received from the field.

b1
b2
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

Name/Foreign Power: (S) [redacted] (S) b1 b6 b7C

b6 , b7C

Declarant: SSA [redacted]

Docket No. & Date Approved: [redacted] (S) b1

Background Facts:

(U) (S) [redacted] b1 b6 b7C (S)

(U) (S) [redacted] (S) b1 b6 b7C

Reason For Initial Application:

(U) (S) [redacted] b1 b6 b7C b7D (S)

(U) (S) [redacted] (S) b1 b2 b6 b7C b7E

(U) (S) [redacted] b1 b2 b6 b7C b7E (S)

(U) 1 (S) [redacted]

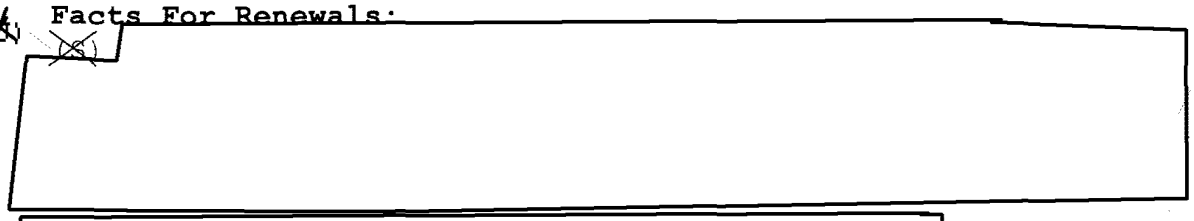
(U) 2 (S) [redacted]

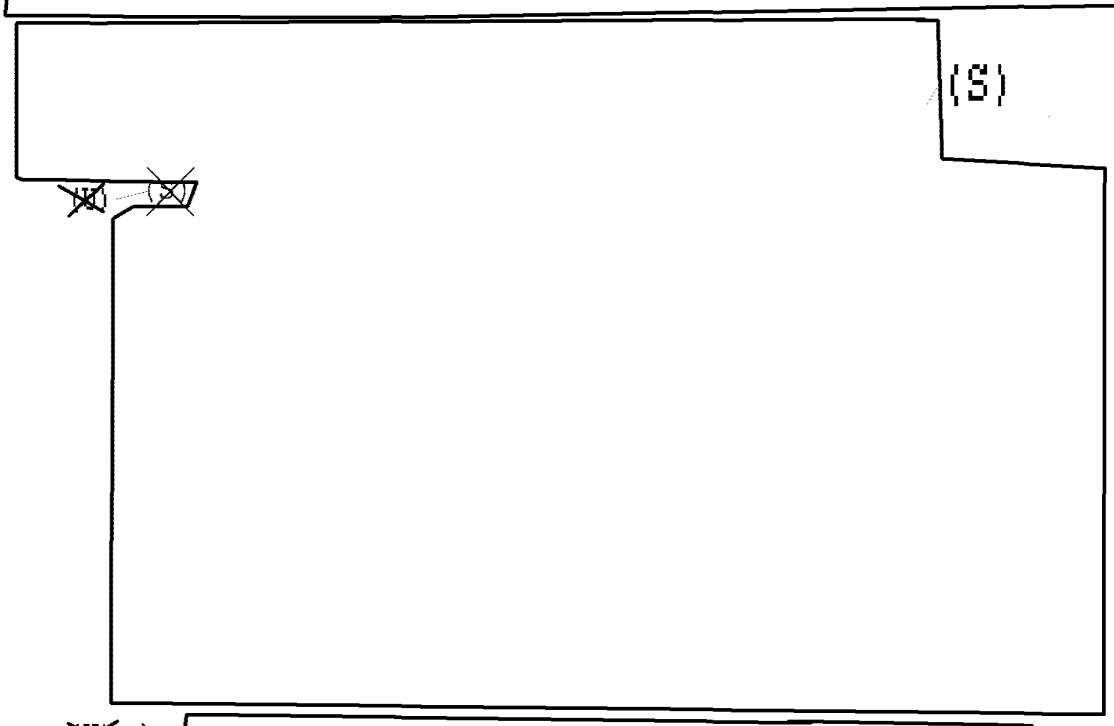
(U) 3 (S) [redacted]

SECRET

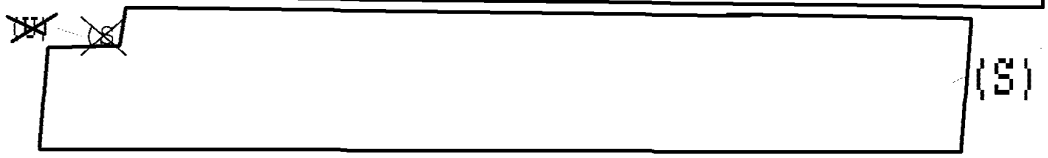
b1
b2
b6
b7C
b7E

Facts For Renewals:



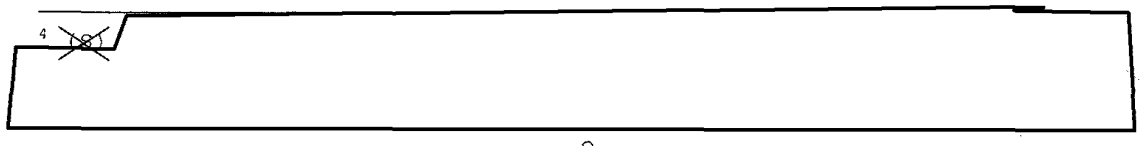


b1
b2
b6
b7C
b7E



b1
b7D

b1
b2
b6
b7A
b7C
b7E



SECRET

SECRET

DATE: 08-18-2005
CLASSIFIED BY 65179/DMH/KBR
REASON: 1.4 (C)
DECLASSIFY ON: 08-18-2030
CA #05-CV-0845

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

b1
b6
b7C

Declarant: b6 b7C SSA SSA

Docket No. & Date Approved:

b1

(S)

b1
b6
b7C

(S)

(S)

b1
b6
b7C

(S)

b1
b6
b7C
b7D

(S)

b1
b2
b6
b7C
b7E

(S)

b1
b2
b7E

(S)

(S)

b1
b2
b6
b7C
b7E

(S)

b1 , b2, b6, b7C, b7E

1 (S)

b1
b6
b7C
b7D

(S)

CA #05-CV-0845
DATE: 08-18-2005
CLASSIFIED BY 65179/DMH/KBR
REASON: 1.4 (C)
DECLASSIFY ON: 08-18-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b6
b7C

(S)

Declarant: SSA
SSA

b6
b7C

Docket No. & Date Approved:

b1

(S)

b1
b6
b7C

(S)

(S)

(S)

b1
b6
b7C

(S/NF)

b1
b6
b7C

(S)

(S/NF)

b1
b2
b6
b7C
b7E

(S)

b1
b2
b6
b7C
b7E

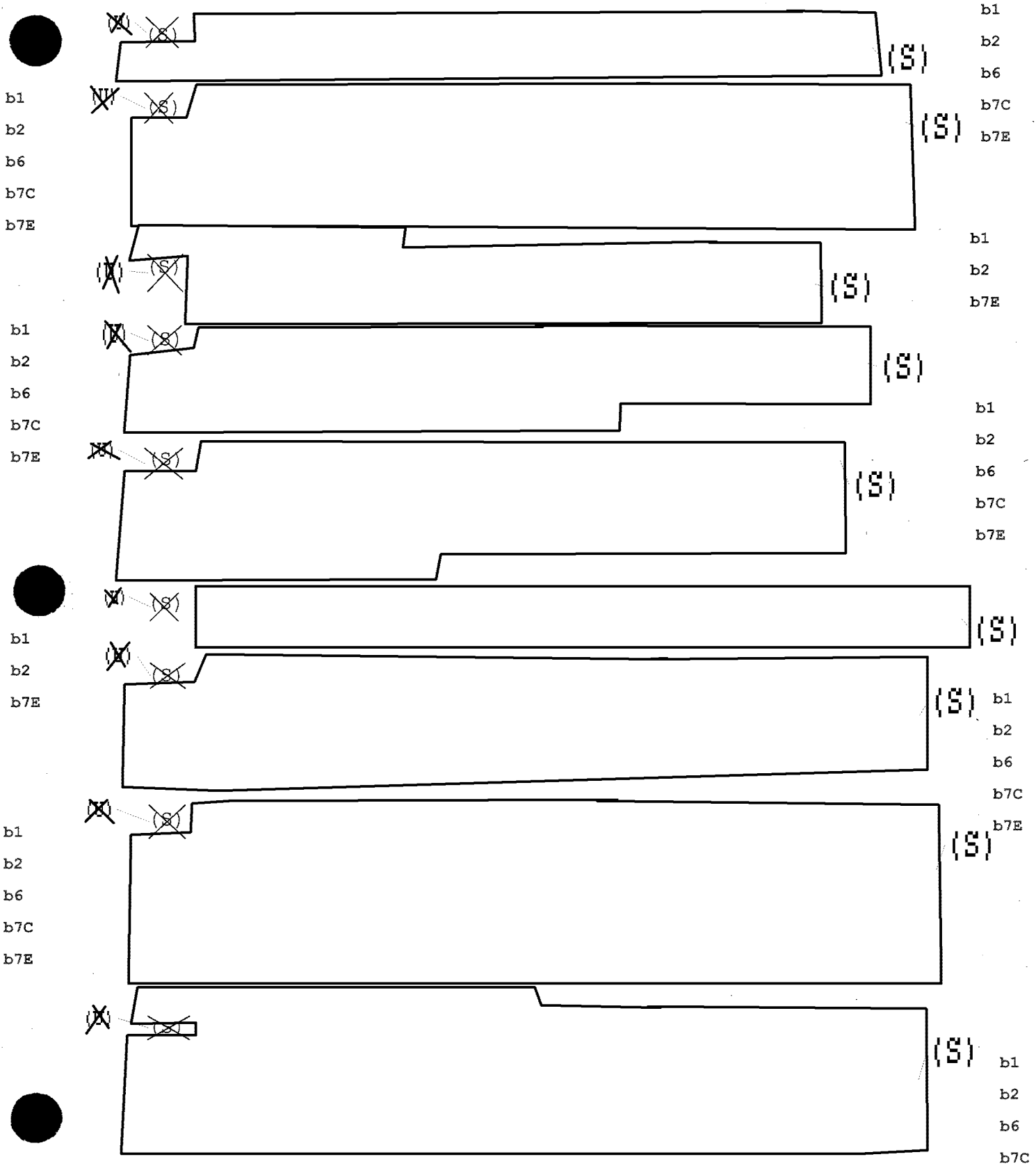
(S)

(S)

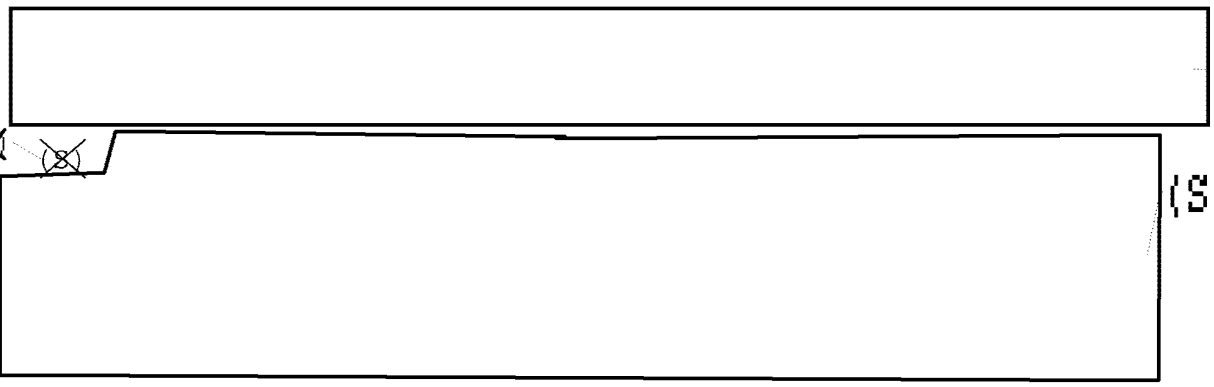
b1
b6
b7C

DATE: 08-18-2005
CLASSIFIED BY 65179/DMH/KBR
REASON: 1.4 (C)
DECLASSIFY ON: 08-18-2030
CA #05-CV-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b1
b2
b7E



b1
b2
b6
b7C
b7E

b1
b6
b7C

(S)

Declarant: SSA

b6 , b7C

b1

(S)

Docket Number and Date Approved:

(S)

(S)

b1
b6
b7C

b1
b6
b7C

(S)

(S)

b1
b6
b7C

b1
b2
b7E

(S)

(S)

b1
b2
b6
b7C
b7E

b1
b6
b7C

[redacted] (S)

Declarant: b6 , b7C SSA [redacted]

Docket No. & Date Approved: [redacted] (S) b1

b1
b6
b7C
b7D

[redacted] (S)

[redacted] (S//OC,NF)

[redacted] (S)

b1
b6
b7C
b7D

[redacted] (S)

b1
b2
b6
b7C
b7E

[redacted] (S)

[redacted] (S)

[redacted] (S)

b1
b2
b6
b7C
b7E

DATE: 08-18-2005
CLASSIFIED BY 65179/DMH/KBR
REASON: 1.4 (B,C,D)
DECLASSIFY ON: 08-18-2030
CA #05-CV-0845

[redacted] (OGC) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, April 14, 2005 2:26 PM
To: [redacted] (OGC) (FBI)
Subject: FW: Roving Authority Example

b6
b7C

SECRET
RECORD xxx-CV-xxxxxxx

-----Original Message-----
From: [redacted] (OGC)(FBI)
Sent: Thursday, April 14, 2005 10:10 AM
To: [redacted] (OGC) (FBI)
Subject: FW: Roving Authority Example

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SECRET
RECORD xxx-CV-xxxxxxx

b6
b7C

[redacted]

This pertains to to the project we talked about this morning.

[redacted]

b6
b7C

-----Original Message-----
From: Caproni, Valerie E. (OGC) (FBI)
Sent: Tuesday, April 12, 2005 3:52 PM
To: [redacted] (CV) (FBI)
Cc: [redacted] (CTD) (FBI); [redacted] (CV) (FBI); [redacted] (OGC) (FBI); [redacted] M (OGC)(FBI)
Subject: RE: Roving Authority Example

SECRET
RECORD xxx-CV-xxxxxxx

Thanks. Were there any tech cuts that you would view as "smoking guns"? or how about just tech cuts that would make a senator say, "ok that is good."

b6
b7C

-----Original Message-----
From: [redacted] CV) (FBI)
Sent: Thursday, April 07, 2005 6:44 PM
To: Caproni, Valerie E. (OGC) (FBI)
Cc: [redacted] (CTD) (FBI); [redacted] (CV) (FBI); [redacted] (OGC) (FBI); [redacted] ERIC M (OGC)(FBI)
Subject: RE: Roving Authority Example

b1
b6
b7C
b7D

SECRET
RECORD xxx-CV-xxxxxxx

[redacted] (S)

b1 , b2, b6, b7C, b7D

(S)

b1 , b2, b5, b6, b7C, b7E

[redacted] (S)

Please contact me if you have any additional questions.

[redacted] b6

Cleveland Division, Canton RA b7C

[redacted] *cell* b2

b6

b7C

-----Original Message-----
From: Caproni, Valerie E. (OGC) (FBI)
Sent: Thursday, April 07, 2005 5:41 PM
To: [redacted](OGC)(FBI); [redacted](OGC) (FBI)
Cc: [redacted]OGC) (FBI); [redacted](OGC) (FBI) [redacted]OGC) (FBI); [redacted](OGC)(FBI); [redacted]OGC) (FBI); [redacted] (CV) (FBI); [redacted](OGC) (FBI)
Subject: RE: Roving Authority Example

~~SECRET~~
RECORD xxx-CV-xxxxxxx

b1
b5
b6
b7C

Great. If you can get a quickie description [redacted] that would be a great example. (S)

-----Original Message-----
From: [redacted](OGC)(FBI)
Sent: Thursday, April 07, 2005 5:37 PM
To: Caproni, Valerie E. (OGC) (FBI); [redacted]OGC) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted] (OGC) (FBI); [redacted](OGC)(FBI); [redacted](OGC) (FBI); [redacted](CV) (FBI) [redacted](OGC) (FBI)
Subject: Roving Authority Example

b6 b7C

b6
b7C

[redacted]

[redacted] (S)

b1
b2
b6
b7C
b7E

[redacted]

[redacted]
Counterintelligence Law Unit
NSLB, OGC JEH Room 7975
[redacted]

b2
b6
b7C

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations~~
~~DECLASSIFICATION EXEMPTION 1~~
~~SECRET~~

b1
b2
b7E

(S)

b1

(S)

(S)

b1
b2
b6
b7C
b7E

(S)

b1
b2
b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET//NOFORN/ORCON~~

(S)

b1
b2
b6
b7C
b7E

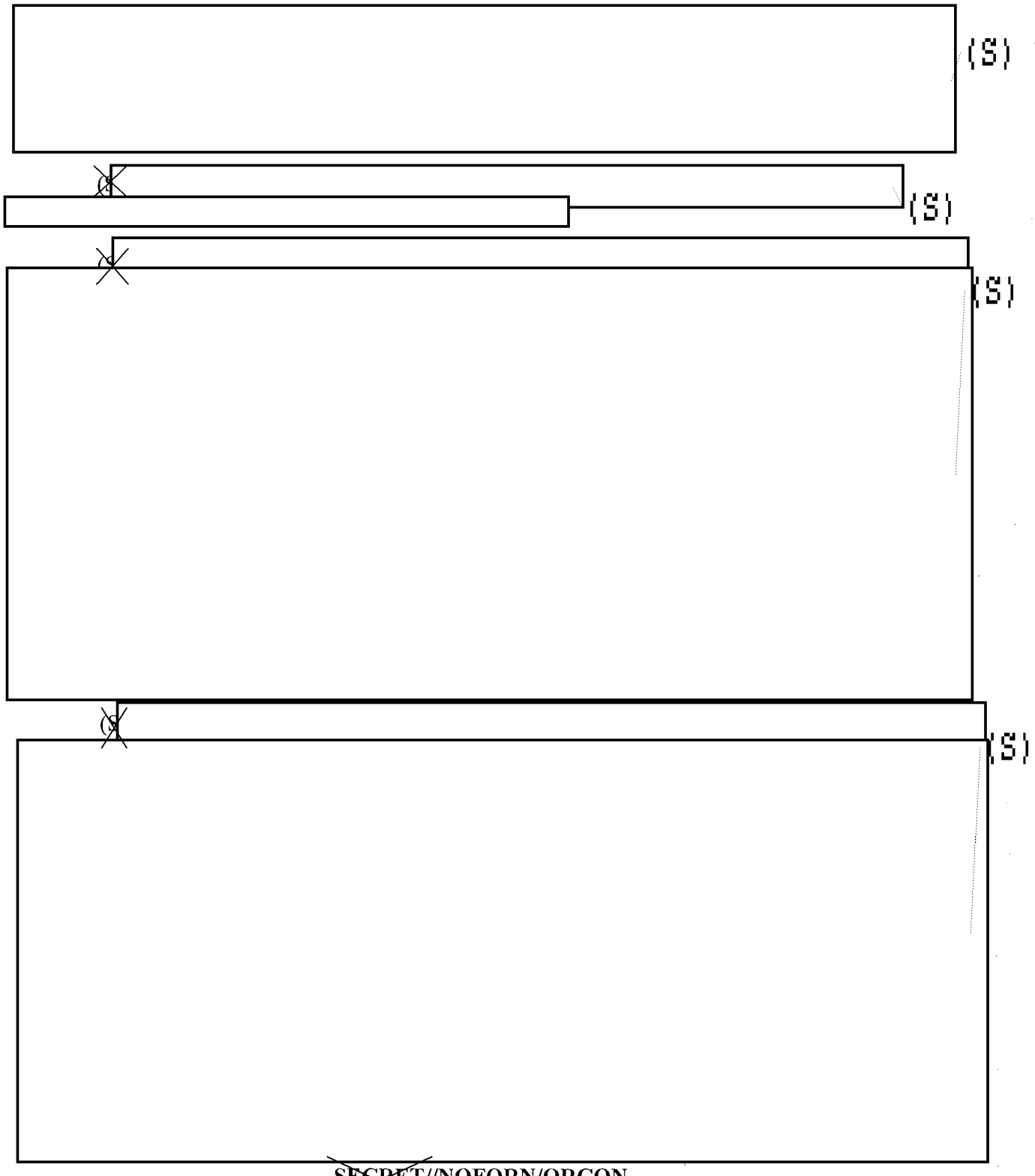
(S)

~~SECRET//NOFORN/ORCON~~

b1 , b2, b3/18 U.S.C. Sec. 3123, b6, b7C

b1 , b2, b3/18 U.S.C. Sec. 3123, b6, b7C, b7E

SECRET//NOFORN/ORCON



SECRET//NOFORN/ORCON

b1 , b2, b3/18 U.S.C. Sec. 3123, b6, b7C, b7E

b1 , b2, b3/18 U.S.C. 3123, b6, b7C, b7E

~~SECRET//NOFORN/ORCON~~

(S)

(S)

b1 , b3/18 U.S.C. Sec. 3123, b6, b7C

(S)

(S)

(S)

b1 , b2, b6, b7C, b7E

b1 , b2, b6, b7C, b7E

(S)

(S)

(S)

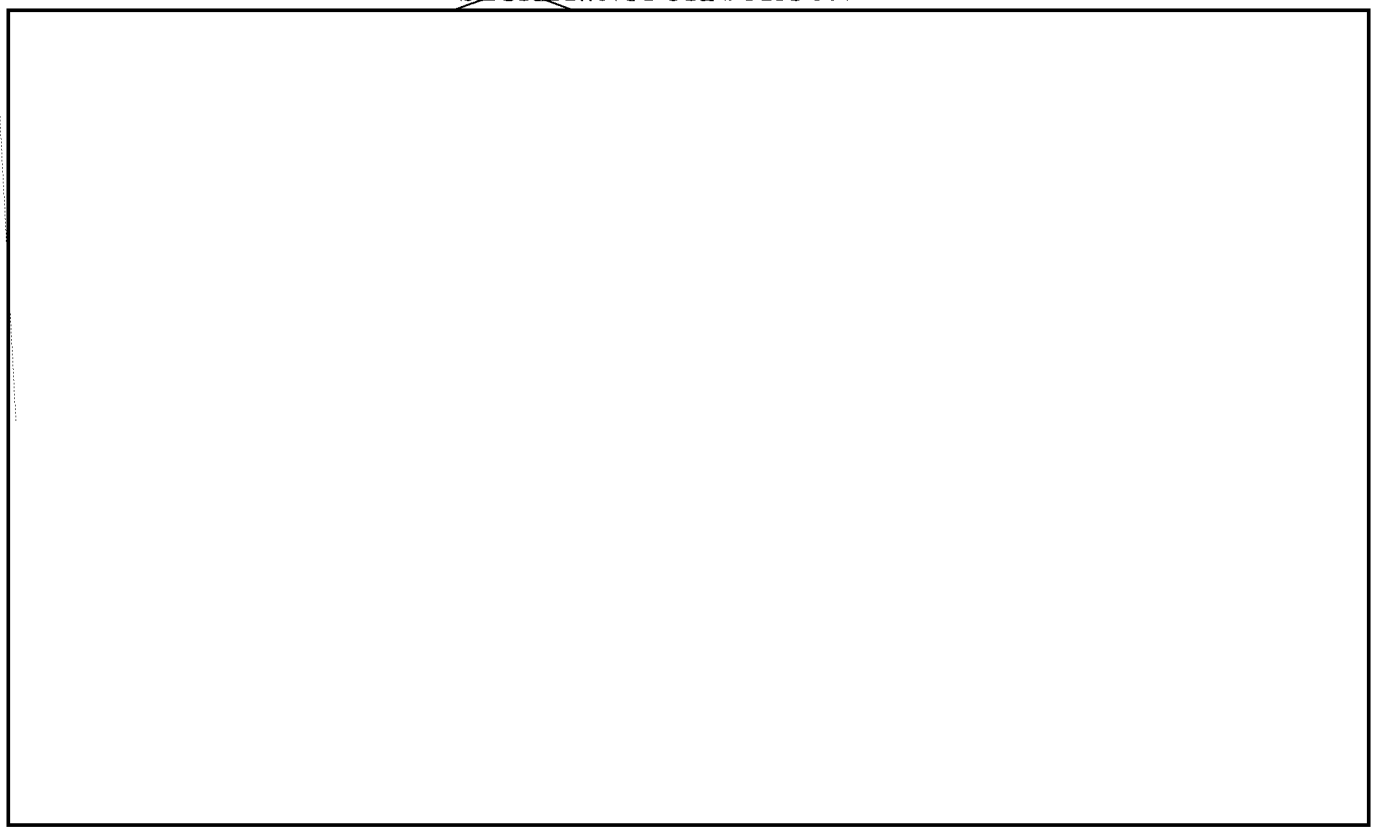
(S)

(S)

(S)

b1 , b2, b6, b7C, b7E

(S)



b1
b2
b7E

[redacted] (S)

[redacted] (S)

b1
b2
b7E

#CA 05-CV-0845

DATE: 08-18-2005
CLASSIFIED BY 65179/DMH/KBR
REASON: 1.4 (C)
DECLASSIFY ON: 08-18-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6 , b7C

[redacted](RMD) (FBI)

From: [redacted](OGC) (FBI)
Sent: Wednesday, June 22, 2005 4:22 PM
To: [redacted](RMD) (FBI) b6
Cc: [redacted](OGC) (FBI) b7C
Subject: EPIC FOIA REQUEST

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I do not believe this was the final version. This is a draft of responses for the Director. I am not sure what the final product looked like.

[redacted] b6 , b7C
Assistant General Counsel
National Security Law Branch
Room 5S-214
[redacted] b2
Ext. [redacted](internal use only)
-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, July 23, 2004 4:48 PM
To: LAMMERT, ELAINE N. (OGC) (FBI) b6
Subject: FW: OGC RESPONSES b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Elaine Lammert:

FYI:

I just spoke with [redacted] He informed me that [redacted] will only be with them for one more week, b2
and he will start working on the responses Monday morning. He stated that he was not familiar with the Patriot b6
Act and need more information on the different sections.
He can be reached at **ext.** [redacted] b7C

[redacted]
Assistant General Counsel
National Security Law Branch
Ext [redacted] b2
-----Original Message-----
From: [redacted](OGC) (FBI) b6
Sent: Friday, July 23, 2004 4:23 PM b7C
To: LAMMERT, ELAINE N. (OGC) (FBI)
Subject: OGC RESPONSES

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Elaine Lammert:

I have attached two versions. One version included (S) as well as (U) examples for the response to question 84f.

The other one only includes (u) unclassified examples.

I did not incorporate [redacted] responses to the other three questions, so they still state that CTD would be able to supply a more detailed response. b6 b7C

[redacted]
Assistant General Counsel
National Security Law Branch
Ext [redacted] b2 b6 b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE HEARING
NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?

b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

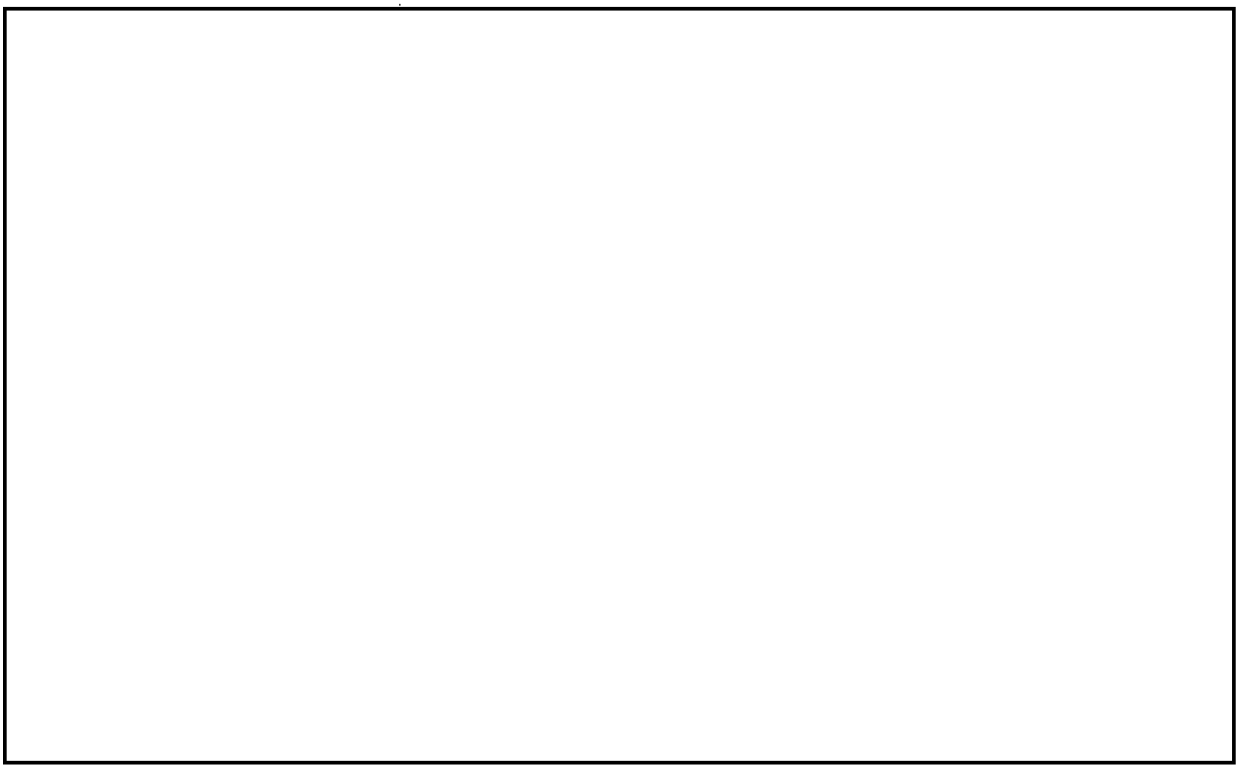
Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors. [redacted]

[redacted] b5

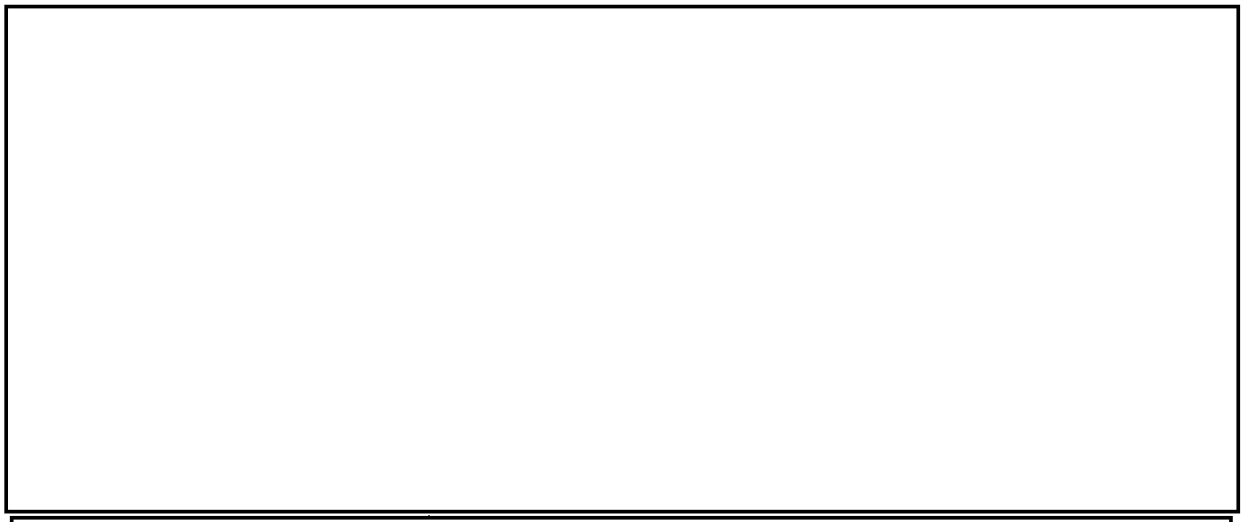
For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?



b5



b5

b5

b5

[redacted] b5

How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

[redacted] b5

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing.

[redacted] b5

b5

55. CTD. (Follow-up to Leahy 15) What specific policy changes have you made in response to the Inspector General's report on 9/11 detainees?

OCA Note: To assist CTD in responding, we note that, in response to a Question for the Record regarding a 9/11 Detainee hearing, the FBI indicated that DOJ and DHS had signed a memorandum of understanding (MOU) related to information sharing and, as recommended by the Inspector General, the FBI was working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. We also indicated that we were working with DHS to establish criteria and procedures for future investigations of alien detainees, including circumstances where a large number of aliens with potential ties to terrorism are detained.

Response: The DOJ and DHS have signed a memorandum of understanding (MOU) relating to information sharing and the FBI is working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. DOJ is still working with DHS to draft an MOU to establish criteria and procedures for future investigations of alien detainees of national security interest. With respect to other policy changes, the FBI has worked to establish the Terrorist Screening Center (TSC) and TTIC, which will substantially improve the FBI's ability to obtain information about alien detainees from various agencies and process this information in a timely fashion. The FBI continues to work with the National Security Law Division, ICE, to review alien detainee cases of national security interest on a case-by-case basis.

58. OGC. (Follow-up to Leahy 18A) When will the FISA Management System (FISAMS) be fully operational? With whom is the contract for development of FISAMS? How much will it cost and what funds are being used to pay for it?

Response: The FISA Management System (FISAMS) became operational at the end of January 2004. The FBI trained the largest 13 FBI field offices on the system. These 13 offices are currently processing their FISA requests through the FISAMS,

which account for approximately 75% of the total FISAs for the FBI. The remaining FBI field offices are in the process of being trained on the FISAMS. [redacted] b5

[redacted]

High Performance Technologies, Inc.(HPTi) is the contractor for the development of the FISAMS. During FY 2003, we currently have allocated $900,000 for Version 1.0 of the FISAMS. We are contracting an additional $1 million with HPTi for enhancements beginning September 2004, which was funded by the Wartime Supplemental Funds received by the FBI. There will be several follow-up versions to further enhance the FISAMS in the future.

[redacted] b5

FY06 is the first budget cycle the FISA Unit has been able to formally request funding for this project.

59. OGC. (Follow-up to Leahy 18C) Did you personally review the 4 FISA applications reportedly not approved by the FISA court last year? Can you provide any details on why the 4 applications were not approved?

[redacted] b5

60. OGC. (Follow-up to Leahy 18D) Can you provide us with a blank copy of the FISA Request Form referenced in your response? Will you provide us with a blank copy of the form that the FBI created for requesting business records from the FISA court?

[redacted] b5

[redacted] b5

[redacted]

b5

61. OGC. (Follow-up to Leahy 21) Did you refer the question to DOJ OIPR? When? Have you been asked to assist in the response? When?

OCA Note: OCA proposes to respond that the FBI forwarded its responses to DOJ on 10/22/03, including our indication that the answer to Senator Leahy's question 21 called for classified information, which is ordinarily supplied to Congress by DOJ's Office of Intelligence Policy and Review (OIPR). By letter to the Committee dated 3/4/04, DOJ's Office of Legislative Affairs forwarded the Department's responses to the Committee, including the FBI's original response to this question.

Response: OGC concurs with OCA's response.

74. CTD. In June 2003, Glenn Fine, the Inspector General for the Justice Department, found "significant problems in the way the detainees were handled" following 9/11. These problems included a failure by the FBI to distinguish between detainees whom it suspected of having a connection to terrorism and detainees with no connection to terrorism; the inhumane treatment of the detainees at a federal detention center in Brooklyn; and the unnecessarily prolonged detention resulting from the Department's "hold until cleared" policy - made worse by the FBI's failure to give sufficient priority to carrying out clearance investigations. In your opinion, has the Justice Department responded in an appropriate manner to all the abuses identified in the Inspector General's report? What steps has the FBI taken to prevent such abuses from occurring in the future?

OCA Note: Based on the responses provided by the FBI to Congressional questions following a hearing regarding the 9/11 detainees, we might begin by noting that, as we have previously advised Congress, the FBI worked diligently to determine whether the detainees, all of whom were in the United States illegally, did, in fact, have terrorism connections. When the FBI was able to determine that an alien was not of interest to the investigation, however, the immigration authorities were notified as soon as possible. While many of the investigations of detainees took longer, for reasons discussed in the Inspector General's report, thorough investigation was necessary to ensure that they posed no danger to our national security. Several steps have been taken to ensure that any future detainee matters are handled as efficiently and effectively as possible. [redacted] As the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). [redacted] b5

Response: The FBI worked diligently to determine whether the detainees, all of whom were in the United States illegally, did, in fact, have terrorism connections. When the FBI was able to determine that an alien was not of interest to the investigation, however, the immigration authorities were notified as soon as possible. While many of the investigations of detainees took longer, for reasons discussed in the Inspector General's report, thorough investigation was necessary to ensure that they posed no danger to our national security.

Several steps have been taken to ensure that any future detainee matters are handled as efficiently and effectively as possible. [redacted] b5

[redacted]

[redacted] **In addition, as the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). For example, an effort is underway to prepare an MOU between DHS and DOJ regarding criteria and procedures for determining alien detainees of national security interest. In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other intitiatives, such as the Foreign Terrorist Tracking Task Force and the National Joint Terrorism Task Force have assisted in permitting better information flow with our law enforcement counterparts and will improve the handling of such cases.** [redacted] b5

[redacted]

82. OGC. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107- 56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeapor[dize] an investigation or unduly [delay] a trial" been used? Please describe the circumstances in each of these cases?

[redacted] b5

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response: This information may be disseminated in any format deemed appropriate for the particular circumstances. [redacted]

[redacted] b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been

issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

[redacted] b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

[redacted] b5

[redacted] b5

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: [redacted] b5 [redacted] **OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information.**

(U) [redacted] b5

[redacted]

(U) [redacted] b5

[redacted] b5

(U)

b5

(U)

b5

(U)

b5

(U)

b5

[redacted] b5

(U) [redacted] b5

(U) [redacted] b5

(U) ~~(S//~~NF,OC) [redacted] b5 b6 b7A b7C

(U) [redacted]

[redacted]

b5
b6
b7C
b7D

(U) [redacted]

b5
b7A
b7D

(U) ~~(S)~~ [redacted]

b5
b7A

(S)

(U) ~~(S)~~ [redacted]

b1
b2
b5
b6
(S) b7C
b7D
b7E

~~SECRET~~

[redacted]

b5
b6
b7C
b7D

~~(S)~~

(S)

[redacted]

b1
b5

(S)

(U) ~~(S)~~

[redacted]

(S)

b1
b5
b6
b7A
b7C

~~(SECRET~~/ORCON/NOFORN)
~~(U)~~

(U) ~~(S)~~

[redacted]

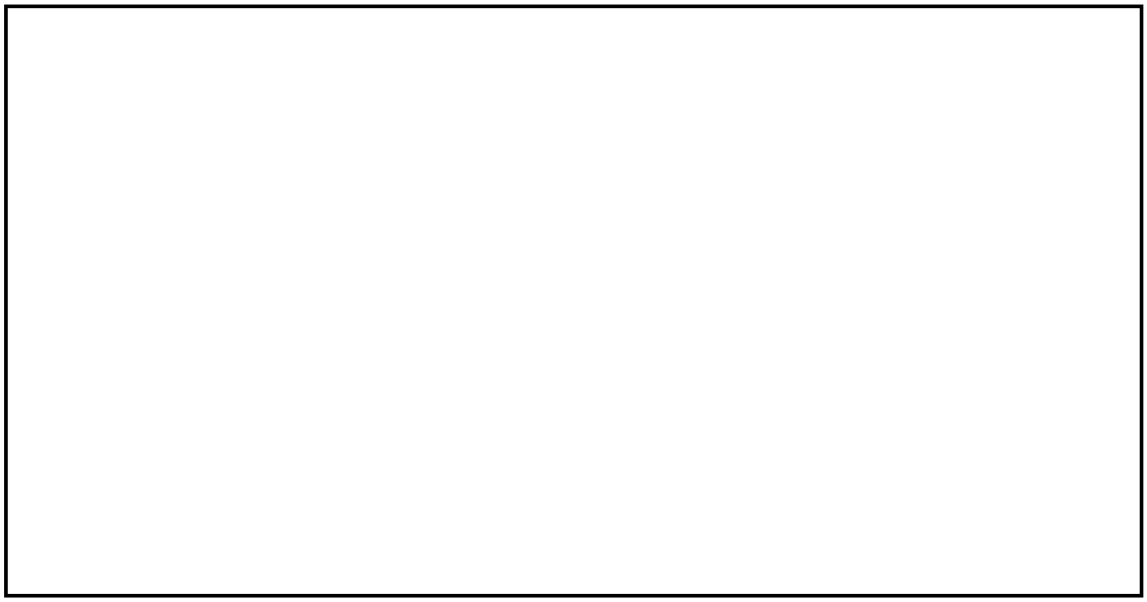
b5
b7A

~~(SECRET~~/ORCON/NOFORN)
(U)

~~SECRET~~

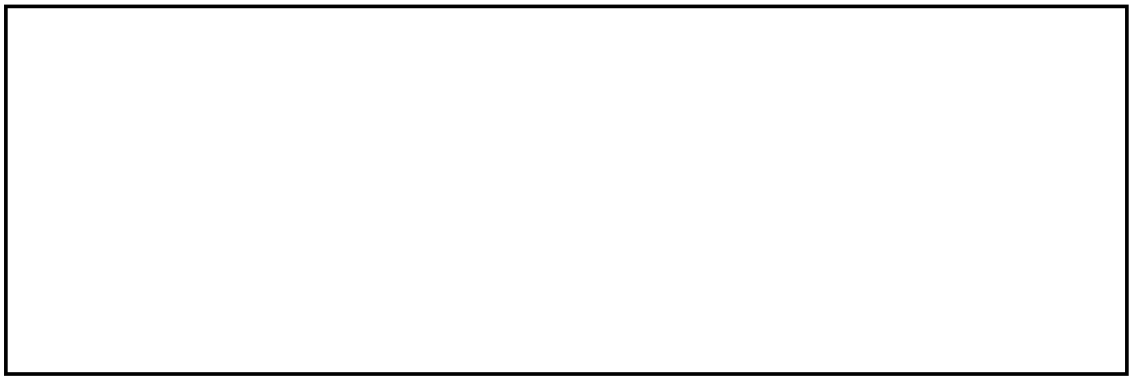
(U)

~~(S)~~



b5
b6
b7A
b7C

(U) ~~(S~~//NF, OC)



b5
b7A

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

b5

b5

[redacted]

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. [redacted] b2 b5 b7E

[redacted]

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community, [redacted] through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins. b5

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence. [redacted] Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area. b5

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners, [redacted] b5

In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, [redacted] **access and responsiveness to local FBI field office, FBI program and national intelligence requirements . The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.** b5

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is

this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

[redacted] b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its

passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

[redacted] b5

(i) How many of such cases were terrorism-related?

[redacted] b5

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

b1
b5
b7A

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

(S)

b5

(S) (U)

b5

(U)

b5

b5

[redacted] b5

[redacted] (U)

[redacted] b5

[redacted] (U)

[redacted] (S)

b1

b5

[redacted] ~~(S)~~ (U)

[redacted]

b5

[redacted] b5

[redacted] b5

[redacted] b5

[redacted] b5

[redacted] b5

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA,

clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

[redacted] b5

[redacted] b5

b5

[redacted]

b1
b5
b7A

[redacted] (S)

[redacted] (S)

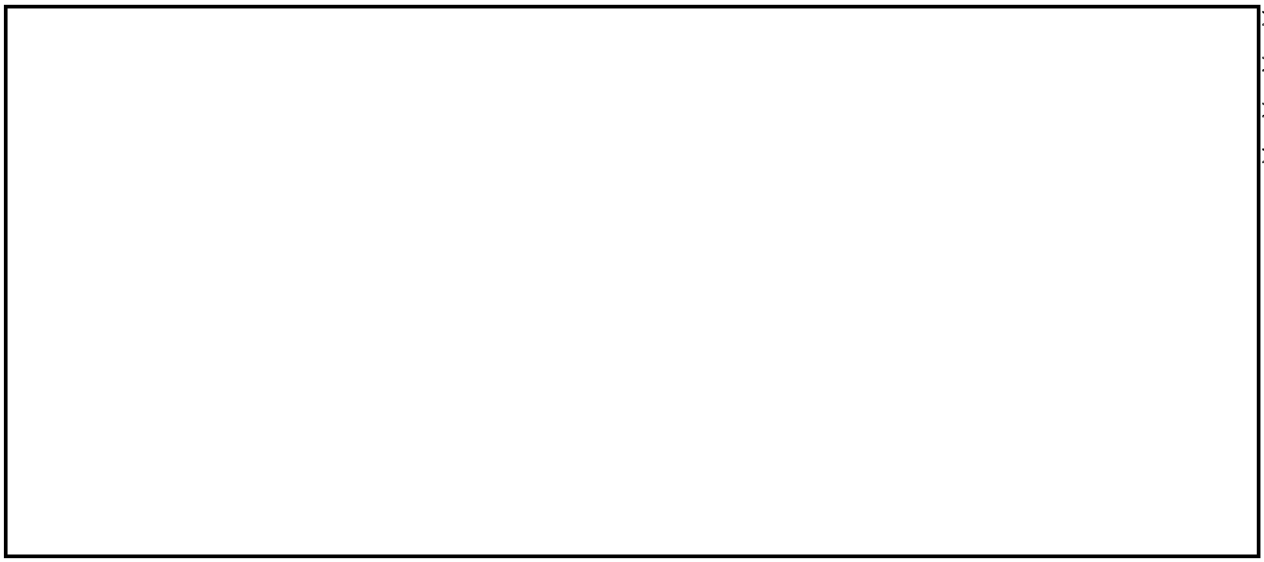
[redacted] (S)

b1
b5
b7A

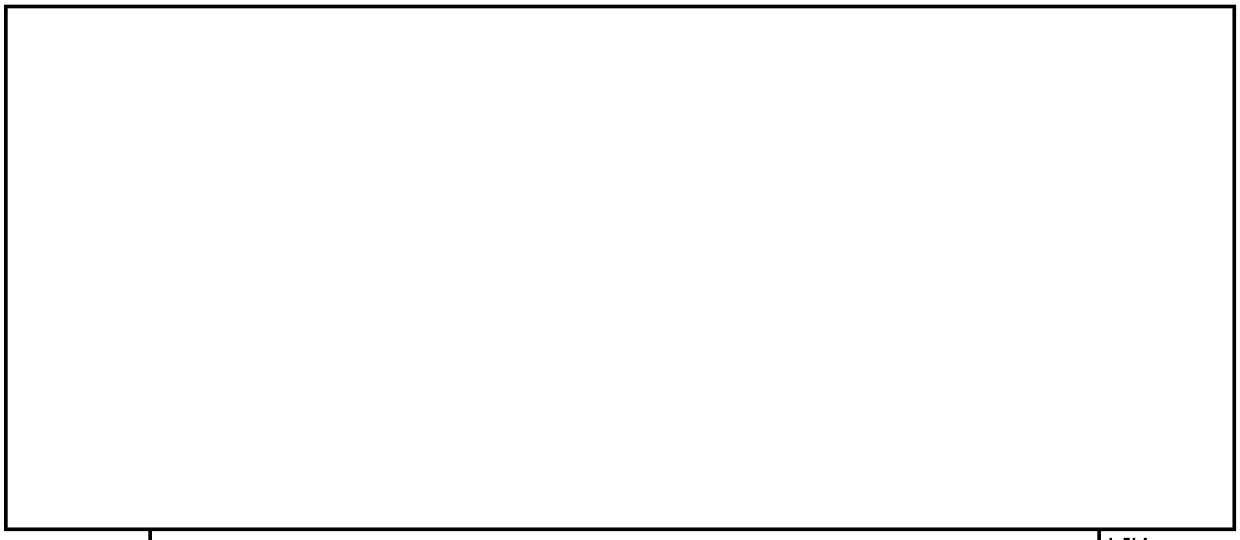
[redacted]

[redacted]

b5
b6
b7C

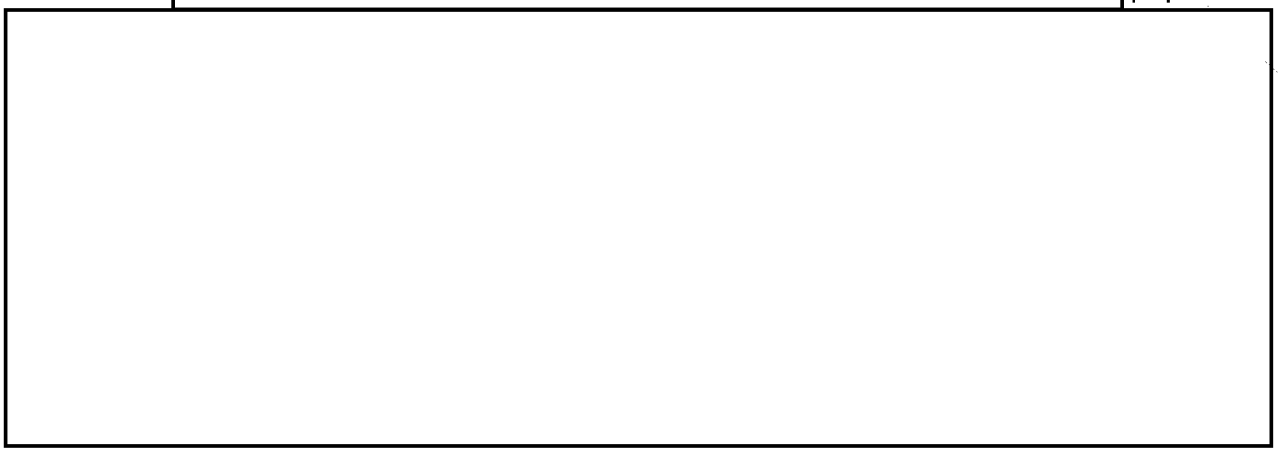


b5
b6
b7C
b7A



b5
b7A

(S)



(S)

b1
b5
b7A

b1
b5
b7A

[redacted] (S)

b5
b6
b7A
b7C

[redacted]

b5
b6
b7C

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

b5

101 d. OGC. According to court records, no criminal charges were

ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

[redacted] b5 b6 b7C

100 e. CTD (in coordination with OGC). Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice. b1 b5 b6 b7C

[redacted] (S)

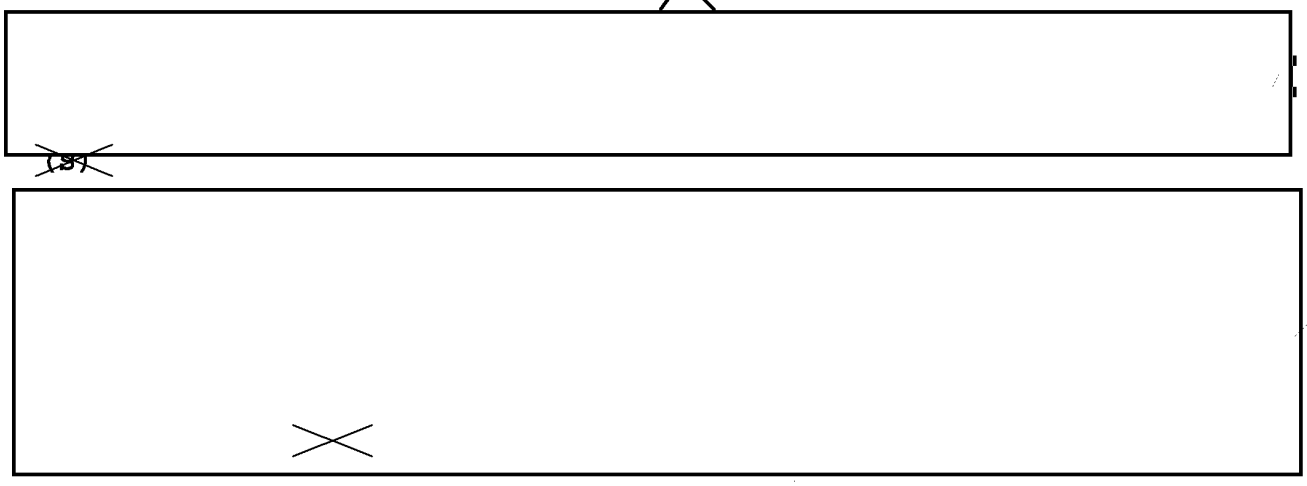
103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

b1
b5
b7A

SECRET



(S)

(S)

(S)

b1
b5
b6
b7A
b7C

SECRET

b6 , b7C

[redacted](RMD) (FBI)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-12-2005 BY 65179 DMH/KJ

05-CV-0845

From: [redacted](OGC) (FBI)
Sent: Wednesday, June 22, 2005 4:27 PM
To: [redacted](RMD) (FBI)
Cc: [redacted](OGC) (FBI)
Subject: FW: NSLB Responses - ~~Secret~~ [OGC seeking assistance from CTD]
(U)
Importance: High

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b6 , b7C

Here is another document that references some of the sections of the Patriot act that is mentioned in the EPIC FOIA request.

[redacted]
Assistant General Counsel
National Security Law Branch
Room 5S-214
[redacted]
Ext. [redacted](internal use only)

b2

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Tuesday, August 03, 2004 11:17 AM
To: LAMMERT, ELAINE N. (OGC) (FBI)
Subject: FW: NSLB Responses - ~~Secret~~ [OGC seeking assistance from CTD]
Importance: High
(U)

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Elaine Lammert:

Here is the whole string of emails. Hopefully you can make sense of it.

[redacted]
Assistant General Counsel
National Security Law Branch
Ext. [redacted]

b2

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Friday, July 23, 2004 2:43 PM
To: [redacted](CTD) (FBI)
Subject: FW: NSLB Responses - ~~Secret~~ [OGC seeking assistance from CTD]
Importance: High
(U)

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

b6
b7C

I just received an Outlook Auto response that [redacted] is out of the office today and possibly Monday. OGC is trying to respond to OCA by COB today.

Would you be able to address the following issues (please see emails below).

Any help would be greatly appreciated.

Thank you in advance,

[redacted]
Assistant General Counsel
National Security Law Branch
Ext. [redacted]

b2

-----Original Message-----
From: [redacted] OGC) (FBI)
Sent: Friday, July 23, 2004 2:39 PM
To: [redacted] (CTD) (OGA)
Subject: FW: NSLB Responses - ~~Secret~~ [OGC seeking assistance from CTD]
Importance: High

b6
b7C

(U)

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

[redacted]

Thank you for your previous help with the questions from OCA. As indicated in my previous email, we unfortunately need more specific answers to the three questions that you so generously provided earlier.

I am sure that you are extremely busy, but OCA is looking for a response no later than COB today. Therefore, any help would be greatly appreciated.

In addition, we wanted to make sure that CTD agrees with our answer to Question 89d, where we state in our response to refer to question 85.

89d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

Please let me know if any of this is possible.

Thank you in advance. Please do not hesitate to contact me for any reason.

b6
b7C

Assistant General Counsel
National Security Law Branch
Ext.

-----Original Message-----
From: OGC) (FBI)
Sent: Wednesday, July 21, 2004 2:41 PM
To: (CTD) (OGA)
Subject: RE: NSLB Responses - ~~Secret~~ (U)

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

Thank you for your responses. Unfortunately, we still have some follow up questions. Question 84 (b) is specific to section 203 (b) which deals with disclosure to grand jury, title 3 etc. Question 84 (d) specifically deals with Section 203 (d) and question 90(e) deals with Section 215 (business records, etc.) of the USA-Patriot Act.

Is it possible to obtain anything more specific?

I appreciate all the help that you have provided with this, and as always any additional information is greatly appreciated.

Please note that I have attached the selected questions to this email.

If you have any questions, please do not hesitate to contact me.

Again, thank you.

b2
b6
b7C

Assistant General Counsel
National Security Law Branch
Ext.

-----Original Message-----
From: (CTD) (OGA)
Sent: Tuesday, July 20, 2004 9:19 AM
To: (OGC) (FBI)
Cc: (CTD) (FBI); (CTD) (FBI)
Subject: RE: NSLB Responses - ~~Secret~~ (U)

b6
b7C

UNCLASSIFIED
NON-RECORD

- you are correct. I believe these questions were all answered in 85.

b6
b7C

Response to 84b: What is the method for disseminating such information to the Intelligence Community?

b5

b2
b5
b7E

b2
b5
b7E

Response to 84c: What is the method for disseminating such information to the Intelligence Community?

b5

[redacted] b5

[redacted] b2 b5 b7E

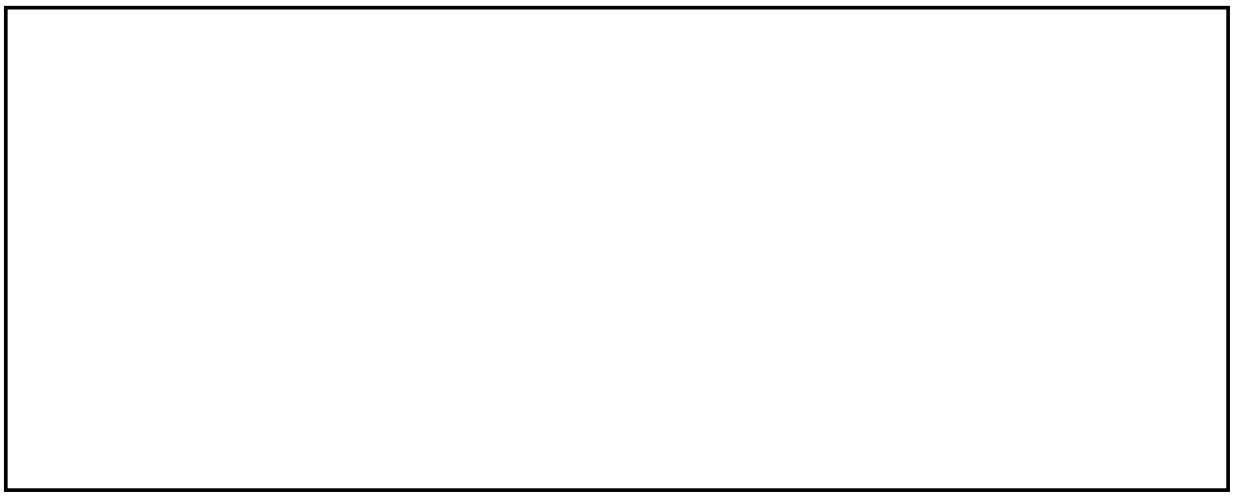
[redacted] b2 b5 b7E

Response to 90e: Is the 'electronic intelligence report" the mechanism used for dissemination of material pursuant to section 215 of the US Patriot Act?

[redacted] b5

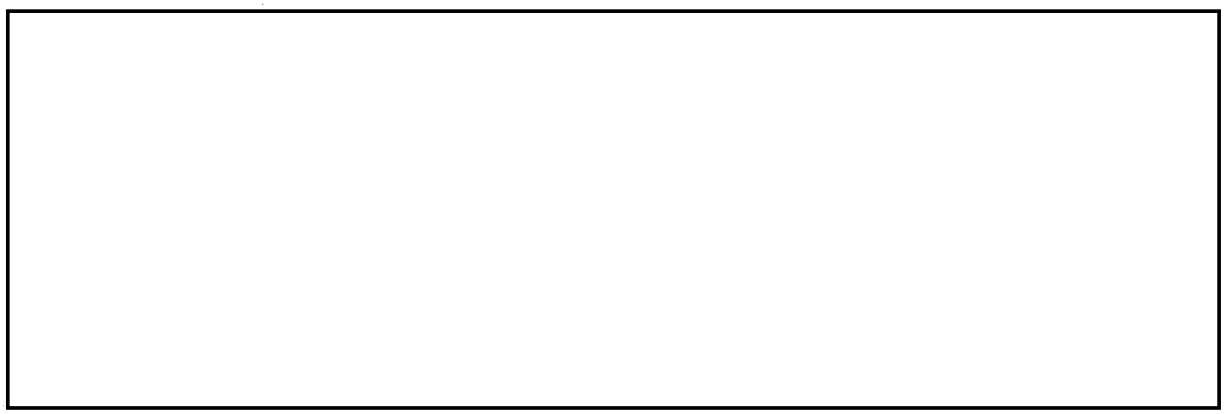
[redacted] b2 b5 b7E

b2
b5
b7E



b2
b5
b7E

(i) If so, how many such reports have been issued?



b5

b5

b5

[redacted] b5

[redacted] b5

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, July 19, 2004 4:34 PM
To: [redacted](CTD) (OGA) b6 b7C
Subject: FW: NSLB Responses - ~~Secret~~
Importance: High (U)

UNCLASSIFIED
NON-RECORD

[redacted]: b6 , b7C

I just left you a message regarding this issue.

NSLB is seeking assistance with three questions posed by OPA/OCA. Elaine Lammert said you are the person with the answers.

NSLB supplied the following attached answers to OPA/OCA. We incorporated the answer that you supplied to question 85. There are three other answers that we thought CTD would be able to answer better/more complete than OGC and indicated such in OGC's responses. (Response to questions 84(b), 84(c), and 90 (e)). We believe that portions of the responses can be found in the answer to 85 that you previously supplied.

OCA stated that they would not accept OGC's answers to 84(b), 84(c), and 90 (e) and that we needed to contact CTD for the answers.

Please let me know if this is possible. Any help is greatly appreciated.

[redacted]
Assistant General Counsel
National Security Law Branch
Ext. [redacted]
-----Original Message-----
From: LAMMERT, ELAINE N. (OGC) (FBI)
Sent: Monday, July 19, 2004 2:50 PM
To: [redacted](OGC) (FBI)
Subject: NSLB Responses - ~~Secret~~

b2
b6
b7C

(U)

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response: This information may be disseminated in any format deemed appropriate for the particular circumstances. b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response: The information may be disseminated in any format deemed appropriate for the circumstances. b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" -

is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE HEARING
NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?

[redacted] b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information,' FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors.

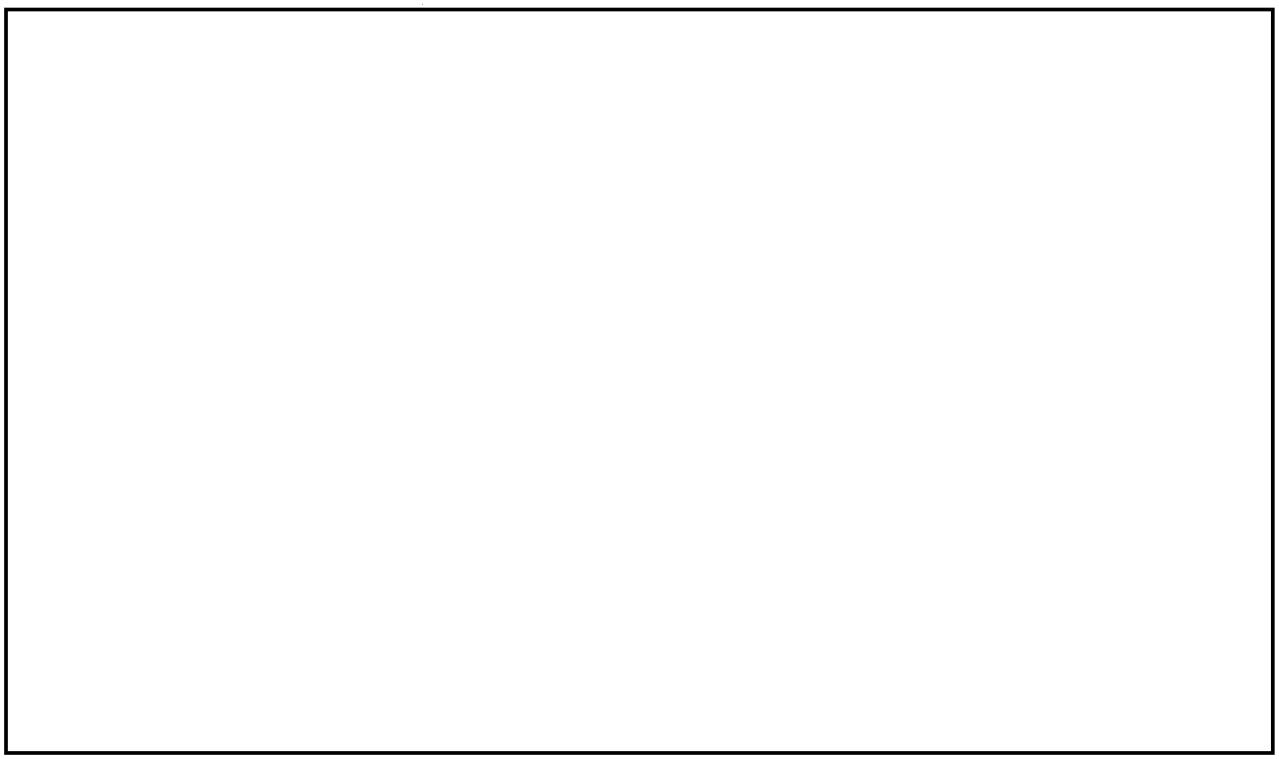
b5

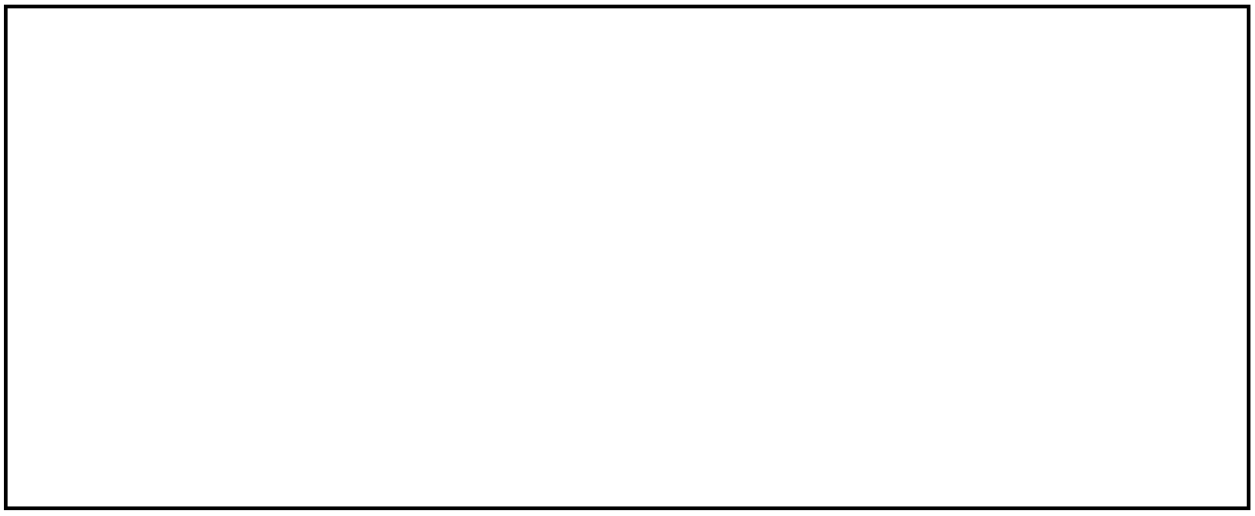
For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?

b5





b5

b5

b5

[redacted] b5

How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

[redacted] b5

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing.

[redacted] b5

b5

55. CTD. (Follow-up to Leahy 15) What specific policy changes have you made in response to the Inspector General's report on 9/11 detainees?

OCA Note: To assist CTD in responding, we note that, in response to a Question for the Record regarding a 9/11 Detainee hearing, the FBI indicated that DOJ and DHS had signed a memorandum of understanding (MOU) related to information sharing and, as recommended by the Inspector General, the FBI was working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. We also indicated that we were working with DHS to establish criteria and procedures for future investigations of alien detainees, including circumstances where a large number of aliens with potential ties to terrorism are detained.

Response: The DOJ and DHS have signed a memorandum of understanding (MOU) relating to information sharing and the FBI is working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. DOJ is still working with DHS to draft an MOU to establish criteria and procedures for future investigations of alien detainees of national security interest. With respect to other policy changes, the FBI has worked to establish the Terrorist Screening Center (TSC) and TTIC, which will substantially improve the FBI's ability to obtain information about alien detainees from various agencies and process this information in a timely fashion. The FBI continues to work with the National Security Law Division, ICE, to review alien detainee cases of national security interest on a case-by-case basis.

58. OGC. (Follow-up to Leahy 18A) When will the FISA Management System (FISAMS) be fully operational? With whom is the contract for development of FISAMS? How much will it cost and what funds are being used to pay for it?

Response: The FISA Management System (FISAMS) became operational at the end of January 2004. The FBI trained the largest 13 FBI field offices on the system. These 13 offices are currently processing their FISA requests through the FISAMS,

b5

which account for approximately 75% of the total FISAs for the FBI. The remaining FBI field offices are in the process of being trained on the FISAMS. [redacted]

[redacted]

High Performance Technologies, Inc.(HPTi) is the contractor for the development of the FISAMS. During FY 2003, we currently have allocated $900,000 for Version 1.0 of the FISAMS. We are contracting an additional $1 million with HPTi for enhancements beginning September 2004, which was funded by the Wartime Supplemental Funds received by the FBI. There will be several follow-up versions to further enhance the FISAMS in the future. b5

[redacted]

FY06 is the first budget cycle the FISA Unit has been able to formally request funding for this project.

59. OGC. (Follow-up to Leahy 18C) Did you personally review the 4 FISA applications reportedly not approved by the FISA court last year? Can you provide any details on why the 4 applications were not approved?

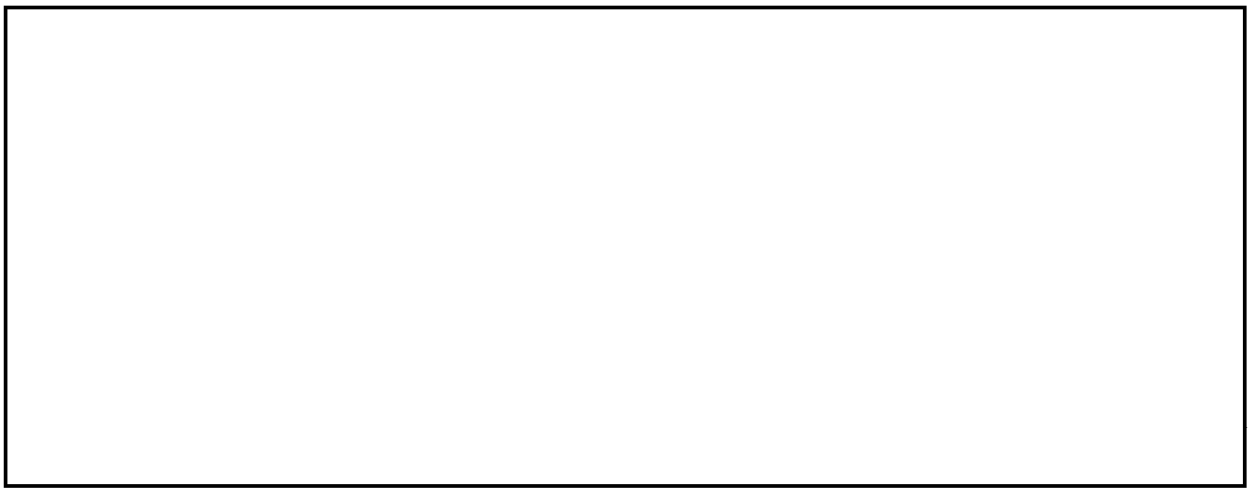
[redacted] b5

60. OGC. (Follow-up to Leahy 18D) Can you provide us with a blank copy of the FISA Request Form referenced in your response? Will you provide us with a blank copy of the form that the FBI created for requesting business records from the FISA court?

[redacted] b5

[redacted]

b5



b5

61. OGC. (Follow-up to Leahy 21) Did you refer the question to DOJ OIPR? When? Have you been asked to assist in the response? When?

OCA Note: OCA proposes to respond that the FBI forwarded its responses to DOJ on 10/22/03, including our indication that the answer to Senator Leahy's question 21 called for classified information, which is ordinarily supplied to Congress by DOJ's Office of Intelligence Policy and Review (OIPR). By letter to the Committee dated 3/4/04, DOJ's Office of Legislative Affairs forwarded the Department's responses to the Committee, including the FBI's original response to this question.

Response: OGC concurs with OCA's response.

74. CTD. In June 2003, Glenn Fine, the Inspector General for the Justice Department, found "significant problems in the way the detainees were handled" following 9/11. These problems included a failure by the FBI to distinguish between detainees whom it suspected of having a connection to terrorism and detainees with no connection to terrorism; the inhumane treatment of the detainees at a federal detention center in Brooklyn; and the unnecessarily prolonged detention resulting from the Department's "hold until cleared" policy - made worse by the FBI's failure to give sufficient priority to carrying out clearance investigations. In your opinion, has the Justice Department responded in an appropriate manner to all the abuses identified in the Inspector General's report? What steps has the FBI taken to prevent such abuses from occurring in the future?

OCA Note: Based on the responses provided by the FBI to Congressional questions following a hearing regarding the 9/11 detainees, we might begin by noting that, as we have previously advised Congress, the FBI worked diligently to determine whether the detainees, all of whom were in the United States illegally, did, in fact, have terrorism connections. When the FBI was able to determine that an alien was not of interest to the investigation, however, the immigration authorities were notified as soon as possible. While many of the investigations of detainees took longer, for reasons discussed in the Inspector General's report, thorough investigation was necessary to ensure that they posed no danger to our national security. Several steps have been taken to ensure that any future detainee matters are handled as efficiently and effectively as possible.

As the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency).

b5

Response: The FBI worked diligently to determine whether the detainees, all of whom were in the United States illegally, did, in fact, have terrorism connections. When the FBI was able to determine that an alien was not of interest to the investigation, however, the immigration authorities were notified as soon as possible. While many of the investigations of detainees took longer, for reasons discussed in the Inspector General's report, thorough investigation was necessary to ensure that they posed no danger to our national security.

b5

Several steps have been taken to ensure that any future detainee matters are handled as efficiently and effectively as possible.

[redacted] In addition, as the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). For example, an effort is underway to prepare an MOU between DHS and DOJ regarding criteria and procedures for determining alien detainees of national security interest. In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other intitiatives, such as the Foreign Terrorist Tracking Task Force and the National Joint Terrorism Task Force have assisted in permitting better information flow with our law enforcement counterparts and will improve the handling of such cases. [redacted]

b5

82. OGC. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107- 56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeapor[dize] an investigation or unduly [delay] a trial" been used? Please describe the circumstances in each of these cases?

b5

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response: This information may be disseminated in any format deemed appropriate for the particular circumstances.

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been

issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

[redacted] b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

[redacted] b5

b5

[redacted]

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: [redacted] **OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information.** [redacted]

b5

[redacted]

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

[redacted]

b5

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. [redacted] b2 b5 b7E

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community, [redacted] through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins. b5

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence. [redacted] Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area. b5

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism

Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners, [redacted] b5

In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, [redacted] **access and responsiveness to local FBI field office, FBI program and national intelligence requirements . The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.** b5

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during

the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

[redacted] b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

b5

[redacted]

(i) How many of such cases were terrorism-related?

[redacted] b5

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non- content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application

of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation

received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider? b1 b5

(S)

b5

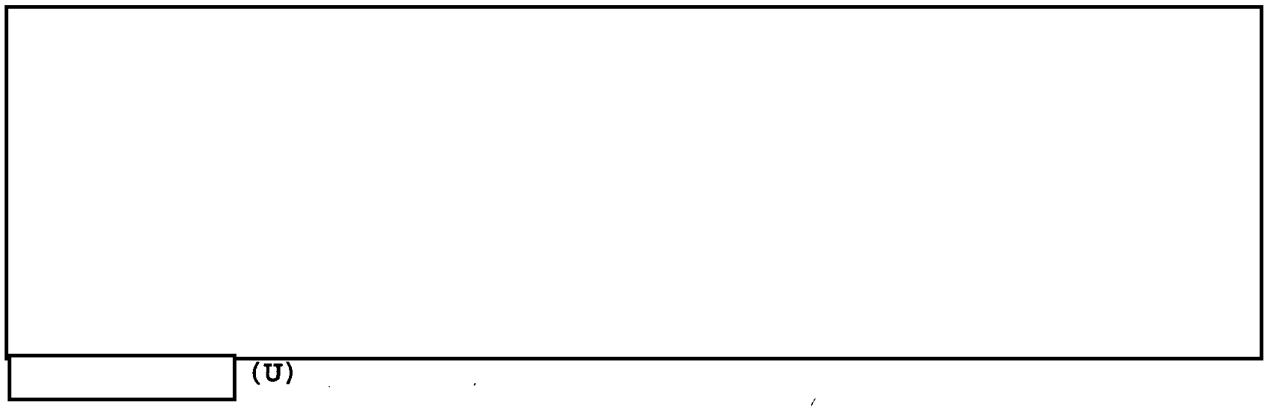
(S) (U)

b5

(U)

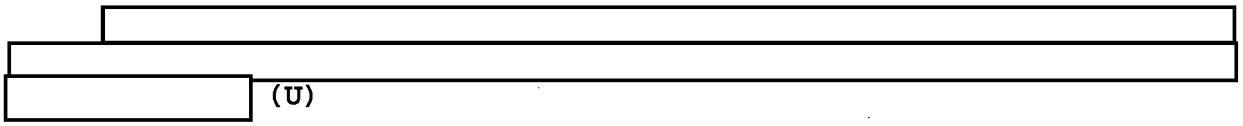
b5

b5



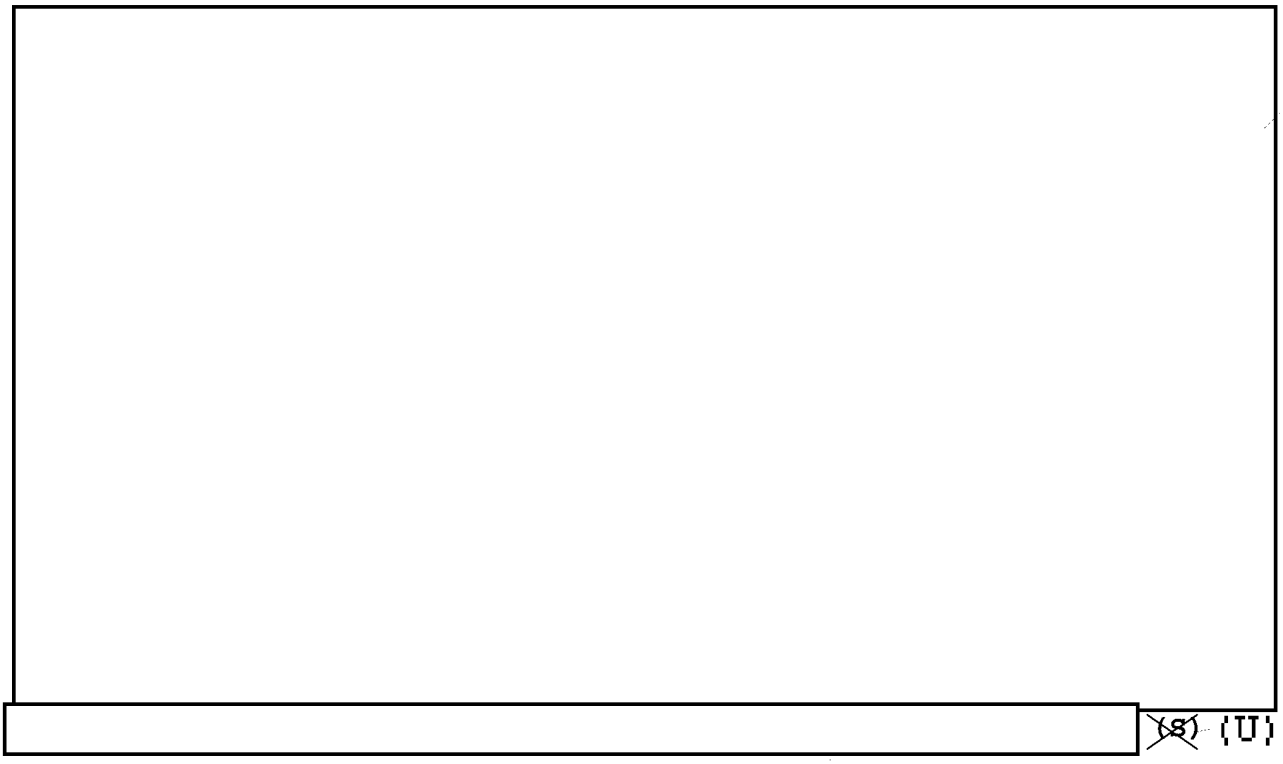
b5

(U)



b5

(U)



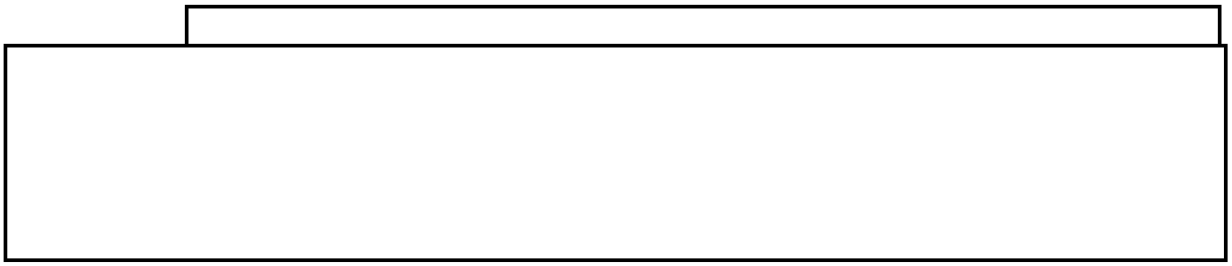
(S)

b1

b5

b7A

(S) (U)



b5

[redacted] b5

[redacted] b5

[redacted] b5

[redacted] b5

[redacted] b5

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation

of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b5

b5

b5

b5

b1
b5
b7A

(S)

(S)

(S)

b1
b5
b7A

b5
b6
b7C

[redacted]

b5
b6
b7A
b7C

[redacted]

b5
b7A

[redacted] (S)

(S)

b1
b5
b7A

b1
b5
b7A

[redacted] (S)

[redacted]

b5
b6
b7A
b7C

[redacted]

[redacted]

b5
b6
b7C

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

[redacted]

b5

101 d. OGC. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

[redacted]

b5
b6
b7C

100 e. CTD (in coordination with OGC). Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.

b1
b5
b6
b7C

[redacted] (S)

103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

b1
b5
b7A

[redacted] (S)

b1
b5
b7A

(S)

(S)

~~TOP~~ SECRET//X1

TO: Mr. James A. Baker
Counsel, Office of Intelligence
Policy and Review

June 5, 2002

FROM: Mr. David W. Szady
Assistant Director
Counterintelligence Division

SUBJECT: [redacted] (U) b2

ACTION MEMORANDUM

[redacted] (S)

b1
b2
b7E

[redacted] (S)

[redacted] (TS)

[redacted] (TS)

1 - [redacted]

[redacted] (2)

b6
b7C

SEE NOTE PAGE 3

DATE: 11-2-2005
CLASSIFIED BY: 65179/DMH/edc
REASON: 1.4(C)
DECLASSIFY ON: 11-2-2030

~~Classified by: 6459, CD-6/CD~~
~~Reason: 1.5 (C)~~
~~Declassify on: X1~~

#05-CV-0845
1017326
FOIPA

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE.

~~TOP~~ SECRET//X1

b1
b2
b7E

Mr. James A. Baker
Counsel, Office of Intelligence Policy and Review
Re: [redacted] (U)

[redacted]

[redacted] (S)

[redacted]

foreign intelligence and counterintelligence. (S)

The point of contact for this matter is Supervisory Special Agent [redacted] FBI Headquarters, Counterintelligence Division, Section CD-6A, telephone number [redacted] (U)

b2
b6
b7C

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 147
Page 2 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 3 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 4 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 5 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 6 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 7 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 8 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 9 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 10 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 11 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 12 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 13 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 14 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 15 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 16 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 17 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 18 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 19 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 20 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 21 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 22 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 23 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 24 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 25 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 26 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 27 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 28 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 29 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 30 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 31 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 32 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 33 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 34 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 35 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 36 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 37 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 38 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 39 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 40 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 41 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 42 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 43 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 44 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 45 ~ b1, b2, b6, b7A, b7C, b7D, b7E

Page 46 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 47 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 48 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 49 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 50 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 51 ~ Referral/Direct
Page 52 ~ Referral/Direct
Page 55 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 56 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 57 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 58 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 59 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 60 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 61 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 62 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 63 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 64 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 65 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 66 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 67 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 68 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 69 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 70 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 71 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 72 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 73 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 74 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 75 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 76 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 77 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 78 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 79 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 80 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 81 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 82 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 83 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 84 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 85 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 86 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 87 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 88 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 89 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 90 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 91 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 92 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 93 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 94 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 95 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 96 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 97 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 98 ~ b1, b2, b6, b7A, b7C, b7D, b7E

Page 99 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 100 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 101 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 102 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 103 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 104 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 105 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 106 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 107 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 108 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 109 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 110 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 111 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 112 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 113 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 114 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 115 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 116 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 117 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 118 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 119 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 120 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 121 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 122 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 123 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 124 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 125 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 126 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 127 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 128 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 129 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 130 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 131 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 132 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 133 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 134 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 135 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 136 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 137 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 138 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 139 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 140 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 141 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 142 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 143 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 144 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 145 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 146 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 147 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 148 ~ b1, b2, b6, b7A, b7C, b7D, b7E
Page 149 ~ b1, b2, b6, b7A, b7C, b7D, b7E

Page 150 ~ b1, b2, b6, b7A, b7C, b7D, b7E

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 10
Page 1 ~ Refer to DOJ, OIPR
Page 2 ~ Refer to DOJ, OIPR
Page 3 ~ Refer to DOJ, OIPR
Page 4 ~ Refer to DOJ, OIPR
Page 5 ~ Refer to DOJ, OIPR
Page 6 ~ Refer to DOJ, OIPR
Page 7 ~ Refer to DOJ, OIPR
Page 8 ~ Refer to DOJ, OIPR
Page 9 ~ Refer to DOJ, OIPR
Page 10 ~ Refer to DOJ, OIPR