

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 4/11/2006

To: All Divisions

Attn: ADIC, AD, DAD, SAC, CDC

From: Office of the General Counsel

National Security Law Branch LX-1 Room 3S100

Contact: [Redacted]

b6
b7C

Approved By: Mueller Robert S III

Drafted By: [Redacted]

Case ID #: [Redacted]

b7E

Title: LEGAL ADVICE AND OPINIONS
BUSINESS RECORD APPLICATIONS
DELEGATION OF AUTHORITY

Reference: [Redacted]

Synopsis: Delegates signature authority for applications for business records for certain types of business record requests to the Deputy Director and the Executive Assistant Director for the National Security Branch under 50 U.S.C. § 1861(a)(3).

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. That delegation was made on 10/10/2003.¹

Under the newly enacted USA PATRIOT Act Improvement and Reauthorization Act of 2005 (2005 PATRIOT Act), the FBI is authorized to issue certain enumerated business record applications only with the approval of the Director or a specified designee:

In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists,

¹ See [Redacted]

To: All Divisions From: Office of the General Counsel
Re: [REDACTED] 04/11/2006

b7E

firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position).² The Deputy Director or the Executive Assistant Director may not further delegate such authority.

50 U.S.C. 1861(a)(3).

DELEGATION OF SIGNATURE AUTHORITY FOR SPECIAL CATEGORIES OF BUSINESS RECORDS REQUESTS

Thus, as permitted by 50 U.S.C. § 1861(a)(3), I hereby delegate certification signature authority for those business record applications enumerated in Section 1861(a)(3) to the following FBI officials:

1. The Deputy Director, and
2. The Executive Assistant Director for the National Security Branch.

CHANGES IN 10/10/2003 DELEGATION AUTHORITY FOR ALL OTHER BUSINESS RECORD REQUESTS

In addition, the prior business records delegation by EC dated 10/10/2003 listed the following officials as having certification signature authority for all business record order applications:³

1. The Deputy Director;

² This position is the Executive Assistant Director for the newly created National Security Branch.

³ The 2005 PATRIOT Act removes certification signature authority for the enumerated applications in Section 1861(a)(3) from these officials; therefore, the 10/10/2003 delegation is modified to recognize that these officials no longer have certification signature authority for such records. Nonetheless, no such business record applications were made under that delegation. In fact, until the passage of the 2005 PATRIOT Act, it was not evident that those records were obtainable via a business record order. The statute now makes clear that those records are in fact obtainable via a business record order.

To: All Divisions From: Office of the General Counsel
Re: [REDACTED] 04/11/2006

b7E

2. The Executive Assistant Director for the Counterterrorism/Counterintelligence;⁴
3. The Assistant Directors 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.⁵

However, in light of changes in FBI organizational structure, I hereby additionally delegate certification signature authority for all business record applications, except those enumerated in Section 1861(a)(3), to

1. The Executive Assistant Director (EAD) for the National Security Branch and the Associate EAD for the National Security Branch; and
2. The Deputy General Counsel for the National Security Law Branch.⁶

FINAL LIST OF FBI OFFICIALS WITH SIGNATURE AUTHORITY FOR ALL OTHER BUSINESS RECORD REQUESTS

Thus, the current list of officials to whom signature authority has been delegated for all but the special categories of business records set forth in Section 1861(a)(3), is as follows:

1. The Deputy Director;
2. The Executive Assistant Director (EAD) and Associate EAD for the National Security Branch;
3. The Assistant Directors and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions;
4. The General Counsel; and

⁴ This position no longer exists in the FBI.

⁵ This position no longer exists in the FBI.

⁶ This position was previously designated as the Deputy General Counsel for National Security Affairs but is more properly termed the Deputy General Counsel for the National Security Law Branch.

To: All Divisions From: Office of the General Counsel
Re: [REDACTED] 04/11/2006

b7E

5. The Deputy General Counsel for the National Security Law Branch.

The National Security Law Branch (NSLB) will continue to issue business record applications for filing with the FISC. Further, NSLB, through its website, will provide further information on the changes made by the 2005 PATRIOT Act to the business records provision of FISA.

To: All Divisions From: Office of the General Counsel
Re: [REDACTED] 04/11/2006

b7E

LEAD:

Set Lead 1: (adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in CI and IT operations and to other personnel as appropriate.

_____ [enter here the overall classification after this form is completed]

**FBI FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)
BUSINESS RECORDS REQUESTS FORM (U)**

INSTRUCTIONS (U)

(U) Use this form to request that the National Security Law Branch (NSLB) _____

b7E

(U) Please direct any questions about this form or _____

(U) Add the overall classification markings to the top and bottom margins and any paragraph classification markings to your answers based on the information you provide.

_____ [enter here the overall classification after this form is completed]

**REQUEST FOR ACCESS TO BUSINESS RECORDS (I.E., ANY
TANGIBLE THING, INCLUDING BOOKS, RECORDS, PAPERS,
DOCUMENTS AND OTHER ITEMS) PURSUANT TO 50 U.S.C. § 1861 (U)**

b7E

(U)



(U)



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-09-2012 BY 65179 DMH/STP/MJS

EXHIBIT A

This page only

~~SECRET~~

DATE: 03-21-2012
FBI INFO.
CLASSIFIED BY 65179 DMH/STP/MJS
REASON: 1.4 (c, d)
DECLASSIFY ON: 03-21-2037

**THE ATTORNEY GENERAL'S GUIDELINES FOR
FBI NATIONAL SECURITY INVESTIGATIONS
AND FOREIGN INTELLIGENCE COLLECTION (U)**

Classified by: John Ashcroft, Attorney General
Reason: 1.4(c)
Declassify on: October 31, 2028.

EFFECTIVE: October 31, 2003

~~SECRET~~

ACLU Sect. 215-1408

~~SECRET~~

PREAMBLE (U)

The following Guidelines on national security investigations and foreign intelligence collection by the Federal Bureau of Investigation (FBI) are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code. They apply to activities of the FBI pursuant to Executive Order 12333 and other activities as provided herein. (U)

~~SECRET~~

~~SECRET~~

TABLE OF CONTENTS (U)

INTRODUCTION 1

A. NATIONAL SECURITY INVESTIGATIONS 2

B. FOREIGN INTELLIGENCE COLLECTION 5

C. STRATEGIC ANALYSIS 5

D. RETENTION AND DISSEMINATION OF INFORMATION 6

I. GENERAL AUTHORITIES AND PRINCIPLES 6

A. GENERAL AUTHORITIES 6

B. USE OF AUTHORITIES AND METHODS 7

C. DETERMINATION OF UNITED STATES PERSON STATUS 9

D. NATURE AND APPLICATION OF THE GUIDELINES 10

II. NATIONAL SECURITY INVESTIGATIONS 11

A. THREAT ASSESSMENTS 12

B. COMMON PROVISIONS FOR PRELIMINARY AND FULL INVESTIGATIONS 13

C. PRELIMINARY INVESTIGATIONS 15

D. FULL INVESTIGATIONS 16

E. EXTRATERRITORIAL OPERATIONS 17

III. INVESTIGATIVE ASSISTANCE TO STATE, LOCAL, AND FOREIGN GOVERNMENTS 18

~~SECRET~~

~~SECRET~~

A.	STATE AND LOCAL GOVERNMENTS	18
B.	FOREIGN GOVERNMENTS	18
IV.	<u>FOREIGN INTELLIGENCE COLLECTION AND ASSISTANCE TO INTELLIGENCE AGENCIES</u>	19
A.	FOREIGN INTELLIGENCE COLLECTION	19
B.	OPERATIONAL SUPPORT	20
C.	CENTRAL INTELLIGENCE AGENCY AND DEPARTMENT OF DEFENSE ACTIVITIES WITHIN THE UNITED STATES	20
V.	<u>INVESTIGATIVE TECHNIQUES</u>	21
VI.	<u>STRATEGIC ANALYSIS</u>	23
VII.	<u>RETENTION AND DISSEMINATION OF INFORMATION</u>	23
A.	INFORMATION SYSTEMS AND DATABASES	23
B.	INFORMATION SHARING	24
C.	SPECIAL STATUTORY REQUIREMENTS	32
VIII.	<u>DEFINITIONS</u>	33

(U)

~~SECRET~~

~~SECRET~~

INTRODUCTION (U)

Following the September 11, 2001, terrorist attack on the United States, the Department of Justice carried out a general review of existing guidelines and procedures relating to national security and criminal matters. These Guidelines reflect the result of that review. (U)

These Guidelines generally authorize investigation by the FBI of threats to the national security of the United States; investigative assistance by the FBI to state, local, and foreign governments in relation to matters affecting the national security; the collection of foreign intelligence by the FBI; the production of strategic analysis by the FBI; and the retention and dissemination of information resulting from the foregoing activities. This includes guidance for the activities of the FBI pursuant to Executive Order 12333, "United States Intelligence Activities" (Dec. 4, 1981). (U)

The general objective of these Guidelines is the full utilization of all authorities and investigative techniques, consistent with the Constitution and laws of the United States, so as to protect the United States and its people from terrorism and other threats to the national security. As Executive Order 12333 provides, "[t]imely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States," and "[a]ll reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available." At the same time, intelligence gathering activities must be carried out in a "responsible manner that is consistent with the Constitution and applicable law," and information concerning United States persons may be collected, retained, and disseminated "only in accordance with procedures . . . approved by the Attorney General." Executive Order 12333, Preamble, §§ 2.1, 2.3. These guidelines should be implemented and interpreted so as to realize as fully as possible the critical objectives of the Executive Order. (U)

The activities of the FBI under these Guidelines are part of the overall response of the United States to threats to the national security, which includes cooperative efforts and sharing of information with other agencies, including other entities in the Intelligence Community and the Department of Homeland Security. The overriding priority in these efforts is preventing, preempting, and disrupting terrorist threats to the United States. In some cases, this priority will dictate the provision of information to other agencies even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. To the greatest extent possible that is consistent with this overriding priority, the FBI shall also act in a manner to protect other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information. (U)

~~SECRET~~

~~SECRET~~

A. NATIONAL SECURITY INVESTIGATIONS (U)

These Guidelines authorize the investigation by the FBI of threats to the national security. Matters constituting threats to the national security, including international terrorism and espionage, are identified in Part I.A.1. Parts II and V of the Guidelines contain the specific provisions governing the conduct of investigations of these threats. (U)

The investigations authorized by these Guidelines serve to protect the national security by providing the basis for, and informing decisions concerning, a variety of measures to deal with threats to the national security. These measures may include, for example, recruitment of double agents and other assets; excluding or removing persons involved in terrorism or espionage from the United States; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism or espionage; providing threat information and warnings to other federal agencies and officials, state and local governments, and private entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats. In addition, the matters identified by these Guidelines as threats to the national security, including international terrorism and espionage, almost invariably involve possible violations of criminal statutes. Detecting, solving, and preventing these crimes – and in many cases, arresting and prosecuting the perpetrators – are crucial objectives of national security investigations under these Guidelines. Thus, these investigations are usually both “counterintelligence” investigations and “criminal” investigations. (U)

The authority to conduct national security investigations under these Guidelines does not supplant or limit the authority to carry out activities under other Attorney General guidelines or pursuant to other lawful authorities of the FBI. Thus, matters within the scope of these Guidelines, such as crimes involved in international terrorism and the activities of groups and organizations that aim to commit such crimes, may also be investigated under the guidelines for general crimes investigations and criminal intelligence investigations. See the Attorney General’s Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, Part II (general crimes investigations) and Part III.B (terrorism enterprise investigations). Likewise, the authorization of extraterritorial activities under Part II.E of these Guidelines overlaps at a practical level with other guidelines the Attorney General has issued for extraterritorial criminal investigations and use of extraterritorial criminal informants. The requirements under these Guidelines to notify FBI Headquarters and other Department of Justice components and officials concerning the initiation and progress of investigations are intended in part to ensure that activities pursuant to these Guidelines are fully coordinated with investigations and activities under other authorities of the FBI. (U)

Part II of these Guidelines authorizes three levels of investigative activity in national security

~~SECRET~~

~~SECRET~~

investigations: (1) threat assessments, (2) preliminary investigations, and (3) full investigations: (U)

- (1) Threat assessments. To carry out its central mission of preventing the commission of terrorist acts against the United States and its people, the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur. (U)

(U)

Part II.A of these Guidelines accordingly authorizes the proactive collection of information concerning threats to the national security, including information on individuals, groups, and organizations of possible investigative interest, and information on possible targets of international terrorist activities or other national security threats (such as infrastructure and computer systems vulnerabilities). This is comparable to the authorization under Part VI of the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations to engage in information collection for counterterrorism or other law enforcement purposes without any more specific investigative predication. The particular methods allowed in threat assessments are relatively non-intrusive investigative techniques, including obtaining publicly available information, accessing information available within the FBI or Department of Justice, requesting information from other government entities, using online informational resources and services, interviewing previously established assets, non-pretexual interviews and requests for information from members of the public and private entities, and accepting information voluntarily provided by governmental or private entities. ~~(S)~~

In addition to allowing proactive information collection for national security purposes, the authority to conduct threat assessments may be used in cases in which information or an allegation concerning possible terrorist (or other national security-threatening) activity by an individual, group, or organization is received, and the matter can be checked out promptly through the relatively non-intrusive techniques authorized in threat assessments. This can avoid the need to open a formal preliminary or full investigation, if the threat assessment indicates that further investigation is not warranted. In this function, threat assessments under these Guidelines are comparable to the checking of initial leads in ordinary criminal investigations. See the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, Subpart A of the Introduction. (U)

- (2) Preliminary investigations. Preliminary investigations are authorized, generally speaking, when there is information or an allegation indicating that a threat to the national security may exist.

~~SECRET~~

~~SECRET~~

(U) Preliminary investigations may relate to individuals, groups, organizations, and possible criminal violations, as specified in Part II.B. ~~(S)~~

(U) Since the legal predicate for mail opening, physical searches, and electronic surveillance that require a judicial order or warrant generally entails more substantial information or evidence than would be available outside of a full investigation, the Guidelines specify that these methods are not available in preliminary investigations. Otherwise, all lawful investigative techniques may be used in preliminary investigations. A non-exhaustive listing of such techniques, including related review or approval requirements, appears in Part V of these Guidelines. These include all the techniques that may be used in threat assessments; interviews and pretext interviews of the subject of the investigation and other persons; use of previously established assets and recruitment of new assets; physical, photographic, and video surveillance not requiring unconsented entry; mail covers; polygraph examinations; inquiry of law enforcement, intelligence, and security agencies of foreign governments; physical searches not requiring a judicial order or warrant; undercover operations and undisclosed participation in organizations; consensual monitoring of communications, including consensual computer monitoring; National Security Letters; and pen registers and trap and trace devices. ~~(S)~~

(U) Preliminary investigations are limited in duration. They may initially be authorized for up to six months, subject to a possible six-month extension by the responsible field office. Extensions of preliminary investigations that continue beyond a year must be authorized by FBI Headquarters. ~~(S)~~

(U) (3) Full investigations. Full investigations are authorized, generally speaking, when there are specific and articulable facts giving reason to believe that a threat to the national security may exist. Like preliminary investigations, full investigations may relate to individuals, groups, organizations, and possible criminal violations, as specified in Part II.B. ~~(S)~~

(U) All lawful investigative techniques may be used in full investigations. These include, in addition to the techniques authorized in threat assessments and preliminary investigations, nonconsensual mail opening, physical searches, and electronic surveillance that require judicial orders or warrants. ~~(S)~~

In investigating threats to the national security, the FBI may request information from foreign law enforcement, intelligence, and security agencies, and may, in certain circumstances, conduct operations outside of the United States. Part II.E of these Guidelines sets out conditions and approval requirements for extraterritorial activities. As provided in Part II.E, these activities require a request

~~SECRET~~

~~SECRET~~

(U) from or approval of the Director of Central Intelligence or a designee. This requirement ensures that extraterritorial activities under these Guidelines are properly coordinated with other agencies in the Intelligence Community, so that their authorities and capabilities are also brought to bear as appropriate to protect the national security, consistent with Executive Order 12333 or a successor order. ~~(S)~~

The FBI may also provide assistance to state and local governments, and to foreign law enforcement, intelligence, and security agencies, in investigations relating to threats to the national security. Part III of these Guidelines specifies standards and procedures for the provision of such assistance. (U)

B. FOREIGN INTELLIGENCE COLLECTION (U)

The FBI's functions pursuant to Executive Order 12333 §§ 1.6, 1.14, 2.3, and 2.4 include engaging in foreign intelligence collection and providing operational support for other components of the U.S. Intelligence Community. This role is frequently critical in collecting foreign intelligence within the United States because the authorized domestic activities of other intelligence agencies are more constrained than those of the FBI under applicable statutory law and Executive Order 12333. (U)

Part IV of these Guidelines provides standards and procedures for the provision of such assistance by the FBI to other federal intelligence agencies and the collection of foreign intelligence by the FBI. (U)

C. STRATEGIC ANALYSIS (U)

Executive Order 12333 § 1.14(d) states that the FBI shall "[p]roduce and disseminate foreign intelligence and counterintelligence." The Executive Order further provides, in § 1.1(a), that "[m]aximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community." Given the magnitude and potential consequences of terrorist threats and other threats to the national security, it is imperative that the FBI develop and maintain a strong analytic capacity to identify, examine, assess, and appropriately disseminate information concerning terrorist threats and to produce and disseminate other analysis relating to national security matters. (U)

Part VI of these Guidelines accordingly authorizes the FBI to examine and analyze information to produce and disseminate foreign intelligence and counterintelligence. Part VI provides that the FBI may draw on information from any source permitted by law in carrying out this analytic function, and may supplement the information in its possession, for purposes of these analytic activities, through the use of the methods authorized in threat assessments, such as obtaining publicly available information and

~~SECRET~~

~~SECRET~~

checking government records. (U)

D. RETENTION AND DISSEMINATION OF INFORMATION (U)

Part VII of these Guidelines requires the maintenance of adequate records and information relating to investigations and other activities under these Guidelines, and provides standards for the sharing and dissemination of information obtained in such investigations and activities. (U)

Part VII includes, in Subpart B.2, provisions for sharing of information and consultation with other Department of Justice components, which reflect legal reforms and policies adopted by the Attorney General following the September 11, 2001, terrorist attack. Consistent with legal norms and standards of effective management, all relevant components, including the Criminal Division, relevant United States Attorneys' offices, and the Office of Intelligence Policy and Review, must be fully informed about the nature, scope, and conduct of national security investigations and other activities under these Guidelines. The Attorney General can most effectively direct and control such investigations and activities only if all relevant Department of Justice components are able to offer advice and recommendations, both strategic and tactical, about their conduct and goals. The overriding need to protect the United States and its people from terrorism and other threats to the national security requires a full and free exchange of information and ideas. (U)

I. GENERAL AUTHORITIES AND PRINCIPLES (U)

A. GENERAL AUTHORITIES (U)

1. The FBI is authorized to conduct investigations to obtain information concerning or to protect against threats to the national security, including investigations of crimes involved in or related to threats to the national security, as provided in Parts II and V of these Guidelines. Threats to the national security are:
 - a. International terrorism.
 - b. Espionage and other intelligence activities, sabotage, or assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons.
 - c. Foreign computer intrusions.
 - d. Other matters as determined by the Attorney General, consistent with Executive

~~SECRET~~

~~SECRET~~

Order 12333 or a successor order. (U)

2. The FBI is authorized to assist state, local, and foreign governments as provided in Part III of these Guidelines. (U)
3. The FBI is authorized to collect foreign intelligence and to assist federal intelligence agencies as provided in Part IV of these Guidelines. (U)
4. The FBI is authorized to conduct strategic analysis as provided in Part VI of these Guidelines. (U)
5. The FBI is authorized to retain and disseminate information collected pursuant to these Guidelines as provided in Part VII of these Guidelines. (U)

B. USE OF AUTHORITIES AND METHODS (U)

1. Protection of National Security (U)

The FBI shall fully utilize the authorities provided and the methods authorized by these Guidelines to protect the national security of the United States. (U)

2. Choice of Methods (U)

The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of information collection methods that are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. As Executive Order 12333 § 2.4 provides, "the least intrusive collection techniques feasible" are to be used in such situations. It is recognized, however, that the choice of techniques is a matter of judgment. The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a threat to the national security or the strength of the information indicating its existence. This point is to be particularly observed in investigations relating to terrorism. (U)

3. Respect for Legal Rights (U)

These Guidelines do not authorize investigating or maintaining information on United

~~SECRET~~

~~SECRET~~

States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. Rather, all activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines. (U)

4. **Relationship to Other Guidelines and Authorities (U)**

- a. The authority to conduct national security investigations and other activities under these Guidelines supplements, and does not supplant or limit, the authority to carry out investigations and other activities under other Attorney General guidelines or pursuant to other lawful authorities of the FBI. These Guidelines accordingly do not limit other authorized law enforcement activities of the FBI, such as those authorized by the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations. (U)
- b. National security investigations and other activities under these Guidelines shall be carried out in conformity with all applicable Executive Branch directives and policies, including Intelligence Community directives and policies, relating to coordination of intelligence activities, information sharing, or other matters. (U)

5. **Maintenance of Records under the Privacy Act (U)**

Under the Privacy Act, the permissibility of maintaining records relating to certain activities of individuals who are United States persons depends in part on whether the collection of such information is "pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. 552a(e)(7). By its terms, the limitation of 5 U.S.C. 552a(e)(7) is inapplicable to activities that do not involve the maintaining of records within the meaning of the Privacy Act, or that occur pertinent to and within the scope of an authorized law enforcement activity. Activities authorized by these Guidelines are authorized law enforcement activities for purposes of the Privacy Act. As noted in paragraph 4. above, these Guidelines do not provide an exhaustive enumeration of authorized law enforcement activities. Questions about the application of the Privacy Act to other activities should be addressed to the FBI Office of the General Counsel or the Department of Justice Office of Information and Privacy. (U)

~~SECRET~~

~~SECRET~~

C. DETERMINATION OF UNITED STATES PERSON STATUS (U)

In some contexts, these Guidelines provide different standards or rules depending on whether investigations or other activities relate to a United States person or to a non-United States person. This Subpart shall be applied in determining whether an individual, group, or organization is a United States person. (U)

1. Meaning of United States Person (U)

A United States person is:

- a. an individual who is a United States citizen or an alien lawfully admitted for permanent residence;
- b. an unincorporated association substantially composed of individuals who are United States persons; or
- c. a corporation incorporated in the United States.

Notwithstanding the foregoing, a foreign power as defined in Part VIII.L.1.-3. of these Guidelines is never to be considered a United States person, including any foreign government or component thereof, any faction of a foreign nation or nations not substantially composed of individuals who are United States persons; or any entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. (U)

b1

2.

(S)

~~SECRET~~

(S)

c.



3. Determination Whether Certain Groups are Substantially Composed of United States Persons (U)

In determining whether a group or organization in the United States that is affiliated with a foreign-based international organization is substantially composed of United States persons, the relationship between the two shall be considered. If the U.S.-based group or organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining if it is substantially composed of United States persons. If, however, the U.S.-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States shall be considered in determining whether it is substantially composed of United States persons. (U)

D. NATURE AND APPLICATION OF THE GUIDELINES (U)

1. Status as Internal Guidance (U)

These Guidelines are set forth solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice. (U)

~~SECRET~~

2. **Departures from the Guidelines (U)**

Departures from these Guidelines must be approved by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General. If a departure from these Guidelines is necessary without such prior approval because of the immediacy or gravity of a threat to the national security or to the safety of persons or property and the need to take immediate action to protect against such a threat, the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General shall be notified as soon thereafter as practicable. The FBI shall provide timely written notice of departures from these Guidelines to the Office of Intelligence Policy and Review. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States. (U)

3. **Interpretation (U)**

All significant new legal questions as to the coverage and interpretation of these guidelines will be resolved initially by the Office of Intelligence Policy and Review and reviewed by the Deputy Attorney General or Attorney General as appropriate. (U)

II. **NATIONAL SECURITY INVESTIGATIONS (U)**

The levels of investigative activity in national security investigations are: (1) threat assessments; (2) preliminary investigations; and (3) full investigations. If the available information shows at any point that the threshold standard for a preliminary investigation or full investigation is satisfied, then that level of investigative activity may be initiated immediately, without progressing through more limited investigative stages. (U)

The scope of authorized activities under this Part is not limited to "investigation" in a narrow sense, such as solving particular cases or obtaining evidence for use in particular criminal prosecutions. Rather, these activities also provide critical information needed for broader analytic and intelligence purposes authorized by Executive Order 12333 and these Guidelines to protect the national security, such as strategic analysis under Part VI, dissemination of information to other agencies in the Intelligence Community under Part VII.B, and dissemination of information to appropriate White House officials under Part VII.B. Information obtained at all stages of investigative activity – threat assessments, preliminary investigations, and full investigations – is accordingly to be retained and disseminated for these purposes as provided in these Guidelines, or in FBI policy consistent with these

~~SECRET~~

~~SECRET~~

Guidelines, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. (U)

A. THREAT ASSESSMENTS (U)

The FBI may, without opening a preliminary or full investigation, engage in the following activities to investigate or collect information relating to threats to the national security, including information on individuals, groups, and organizations of possible investigative interest, and information concerning possible targets of international terrorism, espionage, foreign computer intrusion, or other threats to the national security:

- (U) 1. Obtain publicly available information. ~~(S)~~
- (U) 2. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel. ~~(S)~~
- (U) 3. Check records maintained by, and request information from, other federal, state, and local government entities. ~~(S)~~
- (U) 4. Use online services and resources (whether non-profit or commercial). ~~(S)~~
- (U) 5. Interview previously established assets, informants, and cooperating witnesses (not including new tasking of such persons). ~~(S)~~
- (U) 6. Interview or request information from members of the public and private entities (other than pretext interviews or requests). ~~(S)~~
- (U) 7. Accept information voluntarily provided by governmental or private entities. ~~(S)~~

(U) The foregoing methods may also be used, without opening a preliminary or full investigation, to identify potential assets, or to collect information to maintain the cover or credibility of an asset or employee, in connection with activities related to a threat to the national security. ~~(S)~~

~~SECRET~~

B. COMMON PROVISIONS FOR PRELIMINARY AND FULL INVESTIGATIONS (U)

1. Circumstances for Opening an Investigation (U)

The circumstances on which the initiation of a preliminary investigation or full investigation may be based are:

- (U) a. An individual is or may be an international terrorist or an agent of a foreign power. ~~(S)~~
- (U) b. A group or organization is or may be a foreign power or an agent of a foreign power. ~~(S)~~ b1
- (S) c.
- (U) d. An individual, group, or organization is or may be engaging, or has or may have engaged, in activities constituting a threat to the national security (or related preparatory or support activities) for or on behalf of a foreign power. ~~(S)~~
- (U) e. A crime involved in or related to a threat to the national security has or may have occurred, is or may be occurring, or will or may occur. ~~(S)~~
- (U) f. An individual, group, or organization is, or may be, the target of a recruitment or infiltration effort by an international terrorist, foreign power, or agent of a foreign power under circumstances related to a threat to the national security. ~~(S)~~
- (U) g. An individual, group, organization, entity, information, property, or activity is, or may be, a target of international terrorism, espionage, foreign computer intrusion, or other threat to the national security. ~~(S)~~

2. Authorization and Notice (U)

- a. An FBI field office or FBI Headquarters may initiate a preliminary or full investigation. A field office shall notify FBI Headquarters within ten working days of the initiation by the field office of a preliminary or full investigation. The

~~SECRET~~

(U)

notice of initiation of a preliminary or full investigation, whether the investigation is initiated by a field office or FBI Headquarters, shall identify the grounds for the investigation and describe any pertinent sensitive national security matter(s).

~~(S)~~

- b. FBI Headquarters shall provide the notice of the initiation of a preliminary or full investigation to the Office of Intelligence Policy and Review and to the Criminal Division, and the Office of Intelligence Policy and Review shall notify the Attorney General and the Deputy Attorney General. The notice shall be provided to the Office of Intelligence Policy and Review and the Criminal Division within ten working days of receipt of the notice from a field office by FBI Headquarters or initiation of the investigation by FBI headquarters. The FBI shall also provide the notice of initiation to any relevant United States Attorney's office, subject to authorization by the Criminal Division in an espionage case. Exceptions may be adopted to the requirements of this subparagraph as provided in Part VII.B.2.d. (U)
- c. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a preliminary or full investigation. (U)

3. **Investigations of Groups and Organizations** (U)

(U)

- a. Preliminary and full investigations of groups and organizations should focus on activities related to threats to the national security, not on unrelated First Amendment activities. Any information concerning a group or organization that is relevant to the investigation of a threat to the national security may be sought, including information on any relationship of the group or organization to a foreign power; the identity of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances; its geographical dimensions; and its past and future activities and goals. ~~(S)~~
- b. In the course of a preliminary or full investigation of a group or organization, it may appear that investigation of an individual or individuals within or associated with the group or organization is warranted, beyond the investigation of the individual's activities related to the group or organization as part of the investigation of the group or organization. A preliminary or full investigation of such an individual may be initiated whenever the requirements for initiating a

~~SECRET~~

~~SECRET~~

(U) preliminary or full investigation of an individual are satisfied. ~~(S)~~

C. PRELIMINARY INVESTIGATIONS (U)

1. Initiation (U)

A field office or FBI Headquarters may initiate a preliminary investigation:

a. when there is information or an allegation indicating the existence of a circumstance described in Part II.B.1 of these Guidelines, in order to determine whether the basis exists for a full investigation; or

(U) b. in order to identify potential assets, to determine the suitability or credibility of an individual as an asset, or to collect information to maintain the cover or credibility of an asset or employee, in connection with activities related to a threat to the national security. ~~(S)~~

2. Approval Levels (U)

(U) A preliminary investigation initiated by a field office must be approved by the Special Agent in Charge if the investigation involves a sensitive national security matter. Other preliminary investigations may be approved by the Special Agent in Charge or, as authorized by the Special Agent in Charge, by an Assistant Special Agent in Charge or squad supervisor with responsibility for national security investigations. ~~(S)~~

(U) **3. Authorized techniques (U)**

All lawful investigative techniques may be used in preliminary investigations, including the techniques listed in Part V of these Guidelines, other than the techniques described in Part V.17.-18. (mail opening, physical search, or electronic surveillance requiring judicial order or warrant). ~~(S)~~

4. Duration (U)

Preliminary investigations shall be completed within six months of the date of initiation. In a preliminary investigation initiated by a field office, the Special Agent in Charge or, as authorized by the Special Agent in Charge, an Assistant Special Agent in Charge

~~SECRET~~

~~SECRET~~

(U)

responsible for the investigation, may authorize an extension for an additional six-month period if warranted by facts or information obtained in the course of the investigation. An extension of a preliminary investigation beyond the initial one-year period requires FBI Headquarters approval and may be granted in six-month increments. All extensions shall be in writing and include the reason for the extension. If FBI Headquarters approves an extension of a preliminary investigation beyond the initial one-year period, the FBI shall notify the Office of Intelligence Policy and Review and provide to the Office of Intelligence Policy and Review the extension statement (as described in the preceding sentence) within ten working days of the transmittal of the approval to a field office. ~~(S)~~

D. FULL INVESTIGATIONS (U)

1. Initiation (U)

(U)

FBI Headquarters or a field office may initiate a full investigation if there are specific and articulable facts that give reason to believe that a circumstance described in Part II.B.1 of these Guidelines exists. ~~(S)~~

2. Approval Levels (U)

(U)

A full investigation initiated by a field office must be approved by the Special Agent in Charge if the investigation involves a sensitive national security matter. A full investigation of a foreign official or visitor from a threat country may be approved by the Special Agent in Charge or, as authorized by the Special Agent in Charge, by an Assistant Special Agent in Charge or squad supervisor with responsibility for national security investigations. All other full investigations may be approved by the Special Agent in Charge or, as authorized by the Special Agent in Charge, by an Assistant Special Agent in Charge with responsibility for national security investigations. ~~(S)~~

3. Authorized techniques (U)

(U)

All lawful investigative techniques may be used in full investigations, including the techniques listed in Part V of these Guidelines. ~~(S)~~

~~SECRET~~

~~SECRET~~

4. Reports (U)

In addition to the notice concerning the initiation of investigations required under Part II.B.2 of these Guidelines, the FBI shall notify the Office of Intelligence Policy and Review and the Criminal Division at the end of each year a full investigation continues, and shall prepare and provide to the Office of Intelligence Policy and Review and the Criminal Division at that time a summary of the investigation that includes the information described in Part VII.A.2 of these Guidelines as it relates to the investigation. The FBI shall also provide the summary to any relevant United States Attorney's office, subject to authorization by the Criminal Division in an espionage case. The Office of Intelligence Policy and Review shall notify the Attorney General and the Deputy Attorney General concerning full investigations that continue a year or more and the annual summaries in such investigations. Exceptions may be adopted to the requirements of this paragraph as provided in Part VII.B.2.d. (U)

b1

E. EXTRATERRITORIAL OPERATIONS (U)

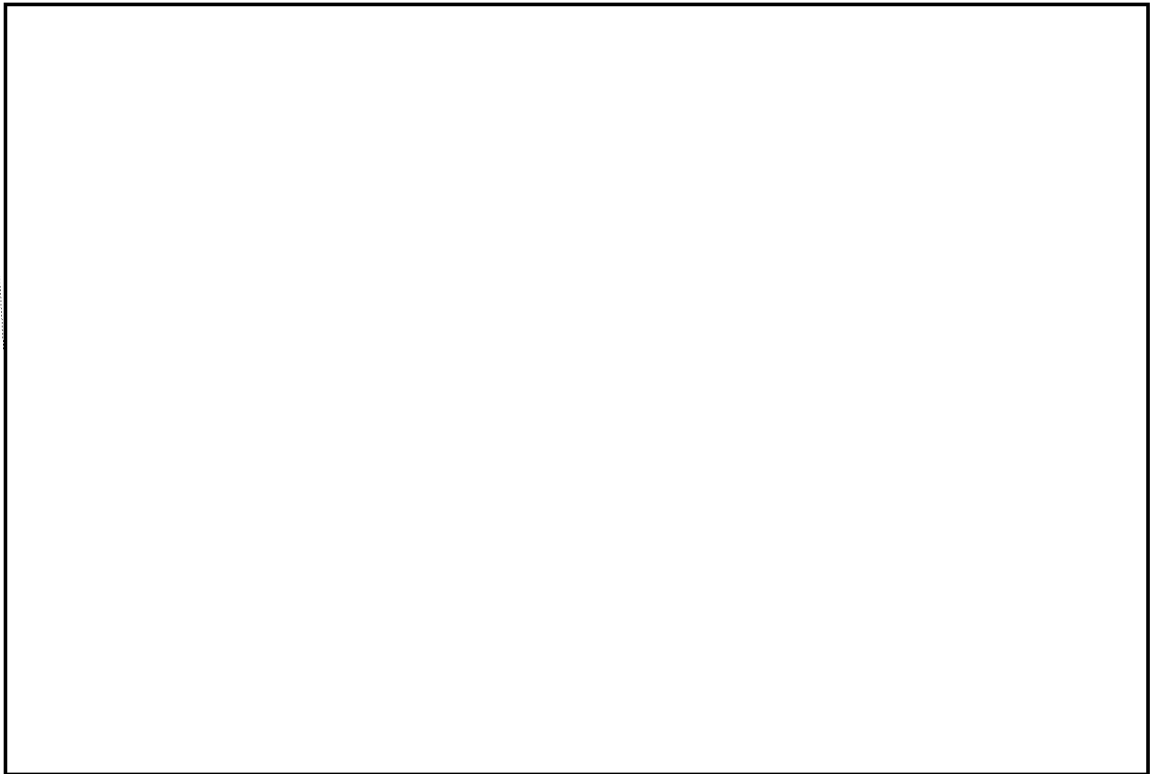
1.

(S)

2.

~~SECRET~~

(S)



3.

III. INVESTIGATIVE ASSISTANCE TO STATE, LOCAL, AND FOREIGN GOVERNMENTS

A. STATE AND LOCAL GOVERNMENTS (U)

The FBI may assist state and local governments in investigations relating to threats to the national security. (U)

B. FOREIGN GOVERNMENTS (U)

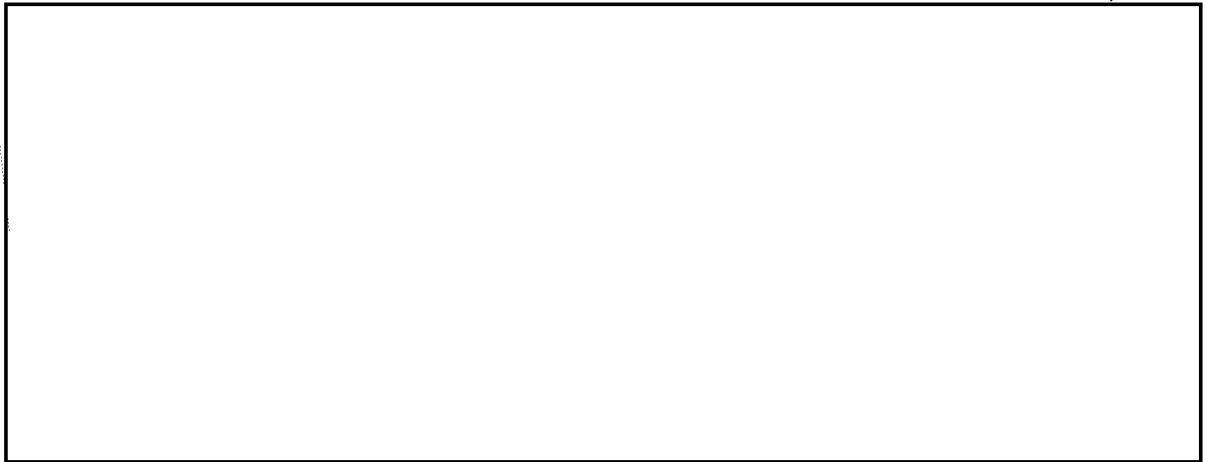
1. The FBI may conduct background inquiries concerning consenting individuals when requested by foreign governments or agencies. (U)

2.

(S)



(S)



3. The FBI may not provide assistance to foreign law enforcement, intelligence, or security officers conducting investigations within the United States unless such officers have provided prior notification to the Department of State as required by 18 U.S.C. 951. (U)
4. The FBI may provide other material and technical assistance to foreign governments to the extent not otherwise prohibited by law. (U)

IV. FOREIGN INTELLIGENCE COLLECTION AND ASSISTANCE TO INTELLIGENCE AGENCIES (U)

A. FOREIGN INTELLIGENCE COLLECTION (U)

1. The FBI may collect foreign intelligence in response to requirements of topical interest published by an entity authorized by the Director of Central Intelligence to establish such requirements, including, but not limited to, the National HUMINT Requirements Tasking Center. When approved by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General, the FBI may collect other foreign intelligence in response to tasking specifically levied on the FBI by an official of the Intelligence Community designated by the President. Upon a request by an official of the Intelligence Community designated by the President, the FBI may also collect foreign intelligence to clarify or complete foreign intelligence previously disseminated by the FBI. Copies of such requests shall be provided to the Office of Intelligence Policy and Review. (U)

2. The FBI may also collect foreign intelligence, if consistent with Executive Order 12333 or a successor order, as directed by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General. (U) b1

3.

(S)



B. OPERATIONAL SUPPORT (U)

1. When approved by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General, the FBI may provide operational support to authorized intelligence activities of other entities of the Intelligence Community upon a request made or confirmed in writing by an official of the Intelligence Community designated by the President. The request shall describe the type and duration of support required, the reasons why the FBI is being requested to furnish the assistance, and the techniques that are expected to be utilized, and shall certify that such assistance is necessary to an authorized activity of the requesting entity. (U)
2. The support may include techniques set forth in the approved request and, with the approval of FBI Headquarters, any other technique that does not substantially alter the character of the support. The FBI shall promptly notify the Office of Intelligence Policy and Review of the utilization of any such additional techniques. (U)
3. The FBI may recruit new assets to obtain information or services needed to furnish the requested support, subject to the same standards and procedures applicable to other FBI assets. (U)

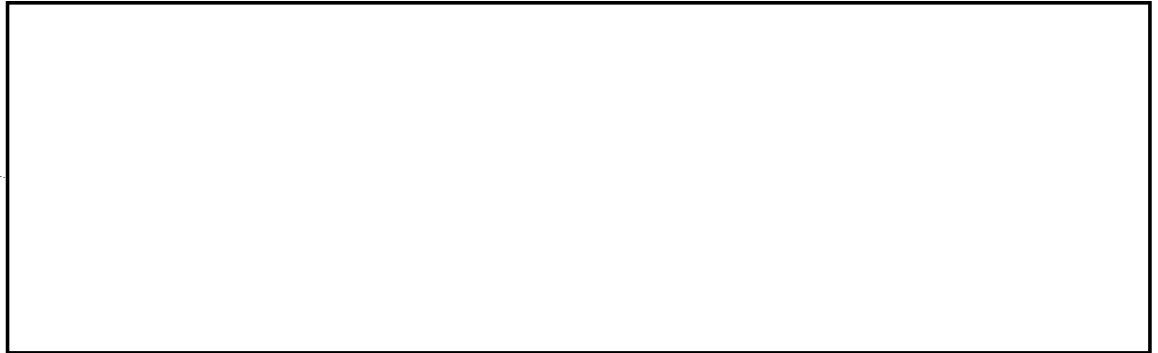
C. CENTRAL INTELLIGENCE AGENCY AND DEPARTMENT OF DEFENSE ACTIVITIES WITHIN THE UNITED STATES (U)

1.

(S)



2.
(S)

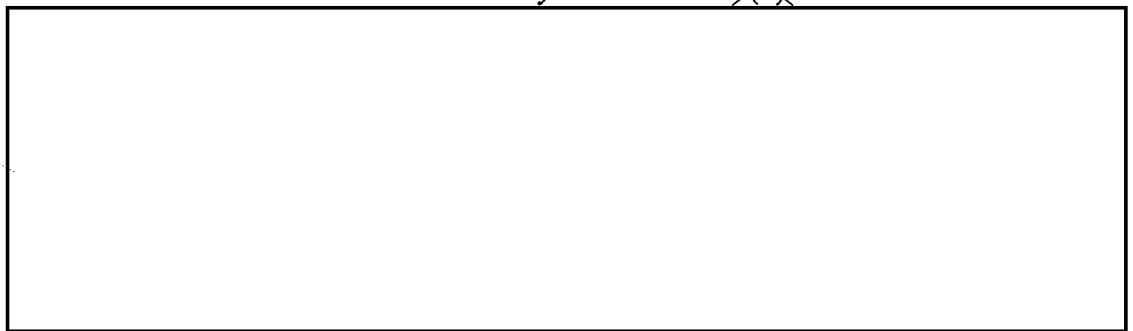


V. INVESTIGATIVE TECHNIQUES (U)

Authorized investigative techniques under these Guidelines include, but are not limited to:

- (U) 1. The techniques authorized in threat assessments under Part II.A. ~~(S)~~
- (U) 2. Interviews and pretext interviews of the subject of an investigation and other persons. ~~(S)~~
- (U) 3. Tasking of previously established assets, informants, and cooperating witnesses, and recruitment of new assets, informants, and cooperating witnesses. ~~(S)~~
- (U) 4. Inquiry of foreign law enforcement, intelligence, or security agencies, and operations outside of the United States in conformity with Part II.E. ~~(S)~~

5.
(S)



- (U) 6. Mail covers. ~~(S)~~
- 7. Physical, photographic, and video surveillance (where such surveillance does not require unconsented entry), including use of such surveillance to identify an individual in

~~SECRET~~

- (U) contact with the subject of a preliminary or full investigation. ~~(S)~~
8. Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers). ~~(S)~~
- (U) 9. Use of closed circuit television, direction finders, and other monitoring devices, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. The methods described in this paragraph usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements. ~~(S)~~
- (U) 10. Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. ~~(S)~~
- (U) 11. Polygraph examinations. ~~(S)~~
- (U) 12. Use of National Security Letters in conformity with 15 U.S.C. 1681u or 1681v (relating to consumer information), 18 U.S.C. 2709 (relating to subscriber information, toll billing records, and electronic communication transactional records), 12 U.S.C. 3414(a)(5)(A) (relating to financial records), or 50 U.S.C. 436 (relating to financial, consumer, and travel records of certain executive branch employees). ~~(S)~~
- (U) 13. Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of title 18, United States Code (18 U.S.C. 2701-2712). ~~(S)~~
- (U) 14. Use of pen registers and trap and trace devices in conformity with FISA (50 U.S.C. 1841-1846) or chapter 206 of title 18, United States Code (18 U.S.C. 3121-3127). ~~(S)~~
- (U) 15. Obtaining business records and other tangible things in conformity with FISA (50 U.S.C. 1861-1863). ~~(S)~~
- (U) 16. Use of grand jury subpoenas and other subpoenas as authorized by law. ~~(S)~~

~~SECRET~~

(U) 17. Electronic surveillance in conformity with chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522), FISA (50 U.S.C. 1801-1811), or Executive Order 12333 § 2.5. ~~(S)~~

b1

(S) 18. 

VI. STRATEGIC ANALYSIS (U)

The FBI may examine and analyze information in its possession in order to produce and disseminate foreign intelligence and counterintelligence. The FBI may draw on information from any source permitted by law in carrying out this function, including any information it has collected or obtained through investigative activities or other activities pursuant to these Guidelines. The FBI may also engage in the activities authorized in threat assessments under Part II.A to supplement information that is otherwise in its possession, for the purpose of carrying out analysis and producing and disseminating foreign intelligence and counterintelligence under this Part. (U)

VII. RETENTION AND DISSEMINATION OF INFORMATION (U)

A. INFORMATION SYSTEMS AND DATABASES (U)

1. The FBI shall retain records relating to preliminary and full investigations, foreign intelligence collection and support activities, and other activities under these Guidelines in accordance with a records retention plan approved by the National Archives and Records Administration. All such records shall be available for review upon request by the Office of Intelligence Policy and Review, including all information in the database or records system described in paragraph 2. (U)
2. The FBI shall maintain a database or records system that permits the prompt retrieval of the following information:

(U) a. The identity and status of each preliminary or full investigation (open or closed), the dates of opening and closing, the predication for the investigation, and whether the investigation involves a United States person. ~~(S)~~

~~SECRET~~

- (U) b. The number of preliminary investigations, the number of preliminary investigations involving United States persons, the number of preliminary investigations involving United States persons in which an extension has been granted, and the number of preliminary investigations that resulted in a full investigation. ~~(S)~~
- (U) c. The number of full investigations and the number of such investigations involving United States persons. ~~(S)~~
- (U) d. The identity of each full investigation of a group in the United States substantially composed of United States persons that is acting for or on behalf of an international terrorist organization. If such an investigation continues a year or more, the annual summary or summaries for the investigation shall include an assessment of the extent to which members of the group are aware of the terrorist aims of the international organization. ~~(S)~~
- (U) e. The number of requests for assistance received from foreign law enforcement, intelligence, or security agencies involving United States persons, and information on the nature of each such request and whether the requested assistance was furnished or declined. ~~(S)~~

B. INFORMATION SHARING (U)

Legal rules and Department of Justice policies regarding information sharing and interagency coordination have been significantly modified since the September 11, 2001, terrorist attack by statutory reforms and new Attorney General guidelines. The general principle reflected in current laws and policies is that information should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. Under this general principle, the FBI shall provide 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. This Subpart provides standards and procedures for the sharing and dissemination of information obtained in national security investigations, foreign intelligence collection, and other activities under these Guidelines. (U)

~~SECRET~~

ACLU Sect. 215-1435

~~SECRET~~

1. General (U)

- a. Information may be disseminated with the consent of the person whom the information concerns, or where necessary to protect life or property from threatened force or violence, otherwise necessary for the safety or security of persons or property or for the prevention of crime, or necessary to obtain information for the conduct of a lawful investigation by the FBI. (U)
- b. Information that is publicly available or does not identify United States persons may be disseminated for any lawful purpose. (U)
- c. Dissemination of information provided to the FBI by other Intelligence Community agencies is subject to applicable agreements and understandings with such agencies concerning the dissemination of such information. (U)

2. Department of Justice (U)

- a. The FBI may share information obtained through activities under these Guidelines with other components of the Department of Justice. (U)
- b. The Criminal Division and the Office of Intelligence Policy and Review shall have access to all information obtained through activities under these Guidelines except as limited by orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, or restrictions established by the Attorney General or the Deputy Attorney General in particular cases. (U)
- c. The FBI shall keep the Criminal Division and the Office of Intelligence Policy and Review apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, subject to the limits noted in subparagraph b. The FBI shall also keep the Criminal Division and the Office of Intelligence Policy and Review apprised of information concerning any crime which is obtained through activities under these Guidelines. (U)
- d. As part of its responsibility under subparagraphs b. and c., the FBI shall provide to the Criminal Division and the Office of Intelligence Policy and

~~SECRET~~

~~SECRET~~

Review notices of the initiation of investigations and annual notices and summaries as provided in Part II.B.2 and .D.4 of these Guidelines, and shall make available to the Criminal Division and the Office of Intelligence Policy and Review relevant information from investigative files. The Criminal Division shall adhere to any reasonable conditions on the storage and disclosure of such documents and information that the FBI and the Office of Intelligence Policy and Review may require. The FBI and the Criminal Division may adopt by mutual agreement exceptions to the provision of notices of the initiation of investigations and annual notices and summaries to the Criminal Division, and the FBI and the Office of Intelligence Policy and Review may adopt by mutual agreement exceptions to the provision of notices of initiation of investigations and annual notices and summaries to the Office of Intelligence and Policy Review. (U)

- e. The FBI, the Criminal Division, and the Office of Intelligence Policy and Review shall consult with each other concerning national security investigations and other activities under these Guidelines, and shall meet regularly to conduct such consultations. Consultations may also be conducted directly between two or more components at any time. Consultations may include the exchange of advice and information on all issues necessary to the ability of the United States to investigate or protect against threats to the national security, including protection against such threats through criminal investigation and prosecution. Consultations are subject to any limitations in orders of the Foreign Intelligence Surveillance Court and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. Disagreements arising from consultations may be presented to the Deputy Attorney General or the Attorney General for resolution. (U)
- f. Subject to subparagraphs g. and h., relevant United States Attorneys' offices shall receive information and engage in consultations to the same extent as the Criminal Division. Thus, the relevant United States Attorneys' offices shall have access to information, shall be kept apprised of information necessary to protect national security, shall be kept apprised of information concerning crimes, shall receive notices of the initiation of investigations and annual summaries as provided in Part II.B.2 and .D.4 of these Guidelines, and shall have access to FBI files, to the same extent as the Criminal Division. The relevant United States Attorneys' offices shall receive such access and

~~SECRET~~

~~SECRET~~

information from the FBI field offices. The relevant United States Attorneys' offices also may and shall engage in regular consultations with the FBI and the Office of Intelligence Policy and Review to the same extent as the Criminal Division. (U)

- g. In espionage cases, dissemination of information to United States Attorneys' offices and consultations between the FBI and United States Attorneys' offices are subject to authorization by the Criminal Division. In an emergency, the FBI may disseminate information to, and consult with, a United States Attorney's office concerning an espionage investigation without the approval of the Criminal Division, but shall notify the Criminal Division as soon as possible thereafter. (U)
- h. Information disseminated to a United States Attorney's office pursuant to subparagraph f. shall be disseminated only to the United States Attorney and/or any Assistant United States Attorneys designated to the Department of Justice by the United States Attorney as points of contact to receive such information. The United States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information. (U)

3. Intelligence Community, Federal Law Enforcement Agencies, and Department of Homeland Security (U)

- a. The FBI shall carry out the requirements of the Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing ("Memorandum of Understanding"), signed by the Attorney General on March 4, 2003. As provided in the Memorandum of Understanding and subject to its provisions, these requirements include timely sharing by the FBI of covered information with other covered entities having a need-to-know, based on a broad interpretation of the missions of the prospective recipients. As used in this paragraph:
 - 1) 'covered entity' has the same meaning as in the Memorandum of

~~SECRET~~

~~SECRET~~

Understanding, including any element of the Department of Homeland Security (and that Department itself); any element of the Intelligence Community (including the Central Intelligence Agency and the Terrorist Threat Integration Center) or of the Department of Justice; and any other entity having federal law enforcement responsibilities;

- 2) 'covered information' has the same meaning as in the Memorandum of Understanding, including terrorism information, weapons of mass destruction information, and vulnerabilities information, as well as analyses based wholly or in part on such covered information;
- 3) 'need-to-know,' 'infrastructure,' 'terrorism information,' 'vulnerabilities information,' and 'weapons of mass destruction information' have the same meanings as in the Memorandum of Understanding; and
- 4) 'timely sharing' of covered information means provision by the FBI of covered information, subject to section 3(h) and other provisions of the Memorandum of Understanding, to other covered entities having a need-to-know: (i) immediately where the FBI reasonably believes that the information relates to a potential terrorism or weapons of mass destruction threat, to the United States Homeland, its infrastructure, or to United States persons or interests, and (ii) as expeditiously as possible with respect to other covered information. (U)

- b. All procedures, guidelines, and mechanisms under the Memorandum of Understanding shall be designed and implemented, and all determinations with regard to sharing information covered by the Memorandum of Understanding shall be made, with the understood, overriding priority of preventing, preempting, and disrupting terrorist threats to the United States. In some cases, this priority will dictate the provision of information even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. However, consistent with this overriding priority, the FBI shall act in a manner to protect, to the greatest extent possible, these other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information. (U)

~~SECRET~~

~~SECRET~~

- c. To the greatest extent possible, information should be shared among covered entities with relevant missions and responsibilities, and there should be transparency among them with regard to their activities to preempt, prevent, and disrupt terrorist attacks against United States persons and interests. Except as otherwise specified in the Memorandum of Understanding, or mandated by relevant federal statutes or Presidential Directives, procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally regardless of the role a particular entity plays as a provider or recipient of covered information. (U)

4. **Federal Authorities (U)**

The FBI may disseminate information obtained through activities under these Guidelines to other federal authorities when:

- a. the information relates to a crime or other violation of law or regulation which falls within the recipient's investigative jurisdiction, or the information otherwise relates to the recipient's authorized responsibilities;
- b. the recipient is a component of the Intelligence Community, and the information is provided to allow the recipient to determine whether the information is relevant to its responsibilities and can be retained or used;
- c. the information is required to be furnished to another federal agency by Executive Order 10450 or its successor; or
- d. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or interagency agreement approved by the Attorney General. (U)

5. **State and Local Authorities (U)**

The FBI may disseminate information obtained through activities under these Guidelines to state and local authorities when:

- a. the information relates to a crime or other violation of law or regulation which falls within the recipient's jurisdiction, and the dissemination is consistent with

~~SECRET~~

~~SECRET~~

national security;

- b. the dissemination is for the purpose of preventing or responding to a threat to the national security, or to public safety, including a threat to the life, health, or safety of any individual or community; or
- c. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or intergovernmental agreement approved by the Attorney General. (U)

6. **Foreign Authorities (U)**

- a. The FBI may disseminate information obtained through activities under these Guidelines to foreign authorities when:
 - 1) the dissemination of the information is in the interest of the national security of the United States, or the information is relevant to the recipient's authorized responsibilities and its dissemination is consistent with the national security interests of the United States, and the FBI has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person; or
 - 2) the information is required to be disseminated by statute or treaty, Presidential directive or executive agreement, National Security Council directive, or Attorney General directive. (U)
- b. Dissemination to foreign authorities having significant implications for foreign relations shall be coordinated with the Department of State. (U)

7. **Congressional Committees (U)**

Except for briefings and testimony on matters of general intelligence interest, information obtained through activities under these Guidelines may be disseminated to appropriate congressional committees when authorized by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General. Any agency requesting or involved in the collection of the information shall be consulted prior to such dissemination. A request for United States person information that has been

~~SECRET~~

~~SECRET~~

withheld from dissemination under this paragraph shall be referred to the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General, for resolution. (U)

8. **White House (U)**

In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the National Security Council and its staff, the Homeland Security Council and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. The FBI accordingly may disseminate information obtained through activities under these Guidelines to the White House, subject to the following standards and procedures: (U)

- a. Requests to the FBI for such information from the White House shall be made through the National Security Council staff or Homeland Security Council staff including, but not limited to, the National Security Council Legal and Intelligence Directorates and Office of Combating Terrorism. (U)
- b. Compromising information concerning domestic officials or political organizations, or information concerning activities of United States persons intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. However, such approval is not required for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House, or concerning contacts by White House personnel with foreign intelligence service personnel. (U)
- c. Examples of types of information that are suitable for dissemination to the White House on a routine basis include, but are not limited to:
 - 1) information concerning international terrorism;

~~SECRET~~

~~SECRET~~

- 2) information concerning activities of foreign intelligence services in the United States;
 - 3) information indicative of imminent hostilities involving any foreign power;
 - 4) information concerning potential cyber threats to the United States or its allies;
 - 5) information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;
 - 6) information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;
 - 7) information concerning foreign economic or foreign political matters that might have national security ramifications; and
 - 8) information set forth in regularly published national intelligence requirements. (U)
- d. The limitations on dissemination of information by the FBI to the White House under these Guidelines do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450. (U)

C. SPECIAL STATUTORY REQUIREMENTS (U)

1. Dissemination of information acquired under the Foreign Intelligence Surveillance Act is subject to minimization procedures approved by the Foreign Intelligence Surveillance Court and other requirements specified in that Act. (U)
2. Information obtained through the use of National Security Letters under 15 U.S.C. 1681v may be disseminated in conformity with the general standards of this Part.

~~SECRET~~

~~SECRET~~

Information obtained through the use of National Security Letters under other statutes may be disseminated in conformity with the general standards of this Part, subject to any applicable limitations in their governing statutory provisions: 12 U.S.C. 3414(a)(5)(B); 15 U.S.C. 1681u(f); 18 U.S.C. 2709(d); 50 U.S.C. 436(e). (U)

VIII. DEFINITIONS (U)

A. AGENT OF A FOREIGN POWER:

1. any person who is not a United States person and who:
 - a. 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; or
 - 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, for or on behalf of a foreign power;
 - d. knowingly enters the United States under a false or fraudulent identity for or on

~~SECRET~~

~~SECRET~~

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

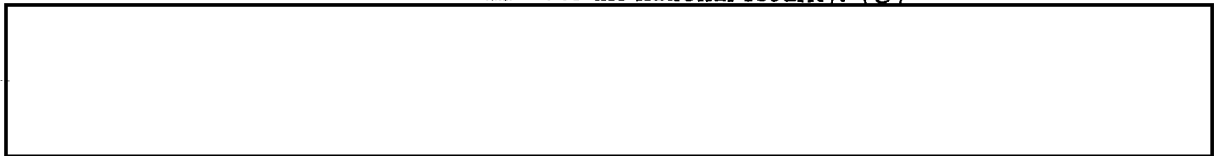
e. knowingly aids or abets any person in the conduct of activities described in subparagraph a., b., or c., or knowingly conspires with any person to engage in such activities. (U)

B. **CONSENSUAL MONITORING OF COMMUNICATIONS:** monitoring of oral, wire, or electronic communications for which a court order or warrant is not legally required because of the consent of a party to the communication. (U)

C. **COUNTERINTELLIGENCE:** information gathered and activities conducted to protect against espionage or other intelligence activities, sabotage, or assassinations conducted by, for or on behalf of foreign powers, organizations or persons; or international terrorist activities, but not including personnel, physical, document or communications security programs. (U)

D. **CRIME INVOLVED IN OR RELATED TO A THREAT TO THE NATIONAL SECURITY:** both crimes directly involved in activities constituting a threat to the national security, and crimes that are preparatory for or facilitate or support such activities. For example, if international terrorists engage in a bank robbery in order to finance their terrorist activities, the bank robbery is a crime involved in or related to a threat to the national security. (U)

(S) E.



b1

F. **FOR OR ON BEHALF OF A FOREIGN POWER:** the determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in:

1. control or policy direction;
2. financial or material support; or
3. leadership, assignments, or discipline. (U)

G. **FOREIGN COMPUTER INTRUSION:** the use or attempted use of any cyber-activity or other means by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into

~~SECRET~~

~~SECRET~~

one or more U.S.-based computers. (U)

- H. FOREIGN CONSULAR ESTABLISHMENT: the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used exclusively by a foreign government for the purposes of a consular post. (U)
- I. FOREIGN DIPLOMATIC ESTABLISHMENT: the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used by a foreign government for the purposes of a diplomatic mission, such as an embassy or other premises and including the residence of the head of the mission; premises of international organizations as defined by 22 U.S.C. 288; premises of establishments authorized to be treated as international organizations or diplomatic missions by specific statute (e.g., 22 U.S.C. 288f-1 to 288h); and the premises of establishments of foreign representatives to such international organizations. (U)
- J. FOREIGN INTELLIGENCE: information relating to the capabilities, intentions, or activities of foreign powers, organizations, or persons, or international terrorist activities. (U)
- K. FOREIGN OFFICIAL: a foreign national in the United States who is acting in an official capacity for a foreign power, attached to a foreign diplomatic establishment, foreign consular establishment, or other establishment under the control of a foreign power, or employed by an international organization or other organization established under an agreement to which the United States is a party. (U)
- L. FOREIGN POWER:
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 person;
 3. an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or government;
 4. a group engaged in international terrorism or activities in preparation therefor;
 5. a foreign-based political organization, not substantially composed of United States

~~SECRET~~

~~SECRET~~

person; or

6. an entity that is directed or controlled by a foreign government or governments. (U)
- M. FOREIGN VISITOR: a foreign national in the United States who is not a permanent resident alien of the United States. (U)
- N. INTELLIGENCE ACTIVITIES: any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power. (U)
- O. INTERNATIONAL TERRORISM:
- 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;
 - 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 be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. (U)
- P. INTERNATIONAL TERRORIST: an individual or group that knowingly engages in international terrorism or activities in preparation therefor, or knowingly aids, abets, or conspires with any person engaged in such activities. (U)
- Q. NATIONAL SECURITY INVESTIGATION: a counterintelligence investigation, pursuant to Part II of these Guidelines, conducted to obtain information concerning or to protect against a

~~SECRET~~

~~SECRET~~

threat to the national security as defined in Part I.A.1. (U)

R. **PHYSICAL SEARCH:** 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 the 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: (1) electronic surveillance as defined in FISA, or (2) the acquisition by the United States Government of foreign intelligence information from international 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 FISA. (U)

S. **PUBLICLY AVAILABLE:** information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could lawfully be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. (U)

T. **RECORDS:** any records, databases, files, indices, information systems, or other retained information. (U)

b1

U.

(S)

V. **SPECIAL AGENT IN CHARGE:** the Special Agent in Charge of a field office, including an Acting Special Agent in Charge. In a field office headed by an Assistant Director, the functions authorized for Special Agents in Charge by these Guidelines may be exercised by the Assistant Director in Charge, or by any Special Agent in Charge as authorized by the Assistant Director in Charge. (U)

W. **STRATEGIC ANALYSIS:** assessment and analysis of information gathered and activities conducted to produce and disseminate foreign intelligence and counterintelligence. (U)

~~SECRET~~

~~SECRET~~

X.




(S)

Y. **UNDISCLOSED PARTICIPATION:** joining or participating in the activities of an organization by an FBI asset or employee without disclosure of FBI affiliation, but not including participation with the knowledge and approval of an official of the organization authorized to act in relation to the activities in question, attendance at an activity open to the public or to acknowledged U.S. Government employees, personal activities not related to FBI employment, or attendance at an academic institution to obtain education or training relevant to FBI employment or to a future undercover role. (U)

Z. **UNITED STATES:** when used in a geographical sense, means all areas under the territorial sovereignty of the United States. (U)

Date: October 31, 2003


John Ashcroft
Attorney General

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/23/2005

To: Counterterrorism Division **Attn:** AD, DAD

Counterintelligence Division AD, DAD

Cyber Division AD, DAD

All Field Offices ADIC
SAC
CDC

From: Office of the General Counsel
National Security Law Branch

Contact: [Redacted]

b6
b7c

Approved By: Caproni Valerie E

[Redacted]

Drafted By: [Redacted]

Case ID #: [Redacted]

b7E

Reference: [Redacted]

Title: LEGAL ADVICE AND OPINIONS;
SERVICE OF CLASSIFIED FISC BUSINESS RECORD ORDERS
ON UNCLEARED CUSTODIANS OF RECORD

Synopsis: Provides guidance to the field in the service of
classified FISC business record orders on uncleared custodians of
records.

Enclosure(s): Revised Business Record Request Form
SAC Approval Form
Model Custodial Trust Receipt
Model Certificate of Service

Details:

Background

The FBI is now able to obtain Business Record Orders
from the Foreign Intelligence Surveillance Court (FISC) under the
Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1861, as
amended by the USA Patriot Act. As set forth in guidance issued

To: Counterterrorism From: Office of the General Counsel
Re: [redacted] 08/23/2005

b7E

by the Office of the General Counsel (OGC) on October 29, 2003,¹ the Patriot Act expanded the scope of the business records the FBI may obtain to include "any tangible things (including books, records, papers, documents, and other items)" and changed the legal standard for issuance of a business record order to one requiring relevance to an authorized national security investigation. Further, as noted in guidance issued by OGC on November 5, 2003,² business record orders may be obtained in preliminary investigations, as well as full investigations, authorized under The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG).³

The business records provision of FISA provides that the FBI applies to the FISC for an order and if it meets the standards of the statute, the judge will enter an ex parte order addressed to the custodian of records for production of the requested material. The FBI and the Office of Intelligence Policy Review (OIPR), U.S. Department of Justice, have agreed in principle upon the format for such an application to the FISC and an order to be issued by the FISC.

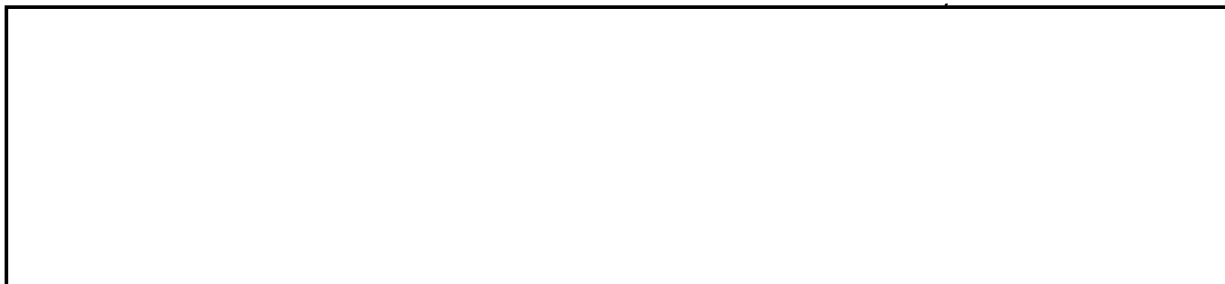
Classified Nature of the Business Record Order

Both the Application that is filed with the FISC and the Order that is subsequently issued by the FISC are classified. The Application will be classified at the level of Secret or above, depending upon the nature of the information contained therein that substantiates the need for the business records. The Order generally will be classified as Secret, based upon the legal theory that there is an inference from its content that

¹ See [redacted]

² See [redacted]

b7E



To: Counterterrorism From: Office of the General Counsel
Re: 08/23/2005

b7E

there is a national security investigation of the subject of the business records, a fact which is classified.⁴

Limited practice has shown that the majority of custodians of records upon whom Orders have been served have neither the necessary clearance to accept them nor the proper storage facilities for storing the classified orders. OGC does not expect this trend to change. Thus, this guidance sets forth the procedures that should be used to allow the recipient of the Order to have access to sufficient information to comply with the Order while at the same time protecting the classified nature of the Order. This guidance is designed to simplify the current practice of serving classified orders upon uncleared persons, inasmuch as it reduces the amount of paperwork that must be generated by the process.

Preliminary Background Check on Custodian of Records

Prior to submission of the business record request form to FBIHQ, the agent who is requesting the business record order ("requesting agent") should have determined who is the appropriate person upon whom to serve the Order. In addition, the agent should have conducted a preliminary background check of the custodian from available databases, such as ACS, NCIC, state and local criminal databases and other appropriate databases.⁵ This will enable the Special Agent in Charge (SAC) to approve the service of the classified Order upon the uncleared custodian of records, assuming no negative or derogatory information came to light during the check.⁶

The Order will name the custodian of records, as set forth in the business record request form, and that person is presumed to be the person upon whom service should be made.

⁴ While the subject of a business record request may not be the target of an investigation, inasmuch as the standard is simply relevance to an authorized investigation, in the vast majority of cases it is expected that in fact the subject of the business record request will be the target of the investigation.

⁵ The newly revised business record request form now provides for the conduct of the preliminary background check on the custodian of records.

⁶ The serving field office may want to have its own SAC approve the service, regardless of whether the requesting field office has done a check and approved the service. In that situation, the serving field office could use a simple form, such as the enclosed SAC Approval form, to document the SAC's approval. There is no need to do a separate electronic communication certifying SAC approval, be it the approval of the requesting field office SAC or serving field office SAC, as is the current practice.

To: Counterterrorism From: Office of the General Counsel
Re: 08/23/2005

b7E

However, the form language of the Order also allows for service upon another unnamed custodian. If a substantial period of time has passed since the business record request form was submitted to NSLB, the identity of the custodian of records should be confirmed. If it is inaccurate, then the requesting agent must determine the identity of and perform a preliminary background check upon the new custodian of records.

Identifying Serving Field Office

Prior to submission of the business record request form, the agent also should have determined the appropriate field office for personal service of the FISC order. If a particular person is known to be the point of contact (POC) in that office for service of the FISC order, that person should also be identified.⁷

Submission of Request to Headquarters, NSLB and FISA Management Unit

As set forth in the OGC Business Record Orders guidance of October 29, 2003, FISC business record order requests should be submitted to the supervisory headquarters operational unit and the National Security Law Branch (NSLB). The request should also be submitted to the FISA Management Unit, for input into its FISA Management System (FISAMS). The FISAMS will route the request through the appropriate approval levels, at the field office and at headquarters.⁸

NSLB will draft the Application and proposed Order for submission to the FISC. Upon approval by OIPR, the Application and proposed Order will be filed with the FISC. When the Order has been issued by the FISC, it will be transmitted to the FISA Unit. In much the same way as FISC Electronic Surveillance

⁷ The newly revised business record request form provides for the identity of the field office that will serve the Order and a POC, if known.

⁸ This procedure applies to requests that are classified SECRET, which are expected to be the vast majority of cases. Because the FISAMS, as of the date of this E.C., can not handle documents classified above the SECRET level, those requests must be transmitted to FBIHQ in paper form, and the field office approvals must be obtained by the requesting agent on the paper copy prior to transmittal to FBIHQ. The newly revised business record request form reflects the fact that these hand-signed approvals at the field office level are not necessary for SECRET requests, since those approvals will be obtained electronically through the FISAMS, but only for requests classified above SECRET. When, as expected, the FISAMS has the capability of handling documents classified above the SECRET level, then the procedure will be the same for all requests.

To: Counterterrorism From: Office of the General Counsel
Re: 08/23/2005

b7E

Orders are handled, the FISA Unit will then forward the Order to the appropriate field office for service.

Serving Classified Order on the Uncleared Custodian of Records

Prior to actually handing the classified FISC order to the custodian of records, the agent from the field office tasked with service of the FISC order ("serving agent") must explain the process to the custodian. Although the custodian of records may have some minimal knowledge about the Order based upon conversations with the requesting agent during the course of obtaining identifying information for the background check, nonetheless, the serving agent should presume the custodian's ignorance of the process. The agent should explain that the custodian has been ordered by a judge of the FISC to comply with an FBI request for the production of business records. In order to facilitate compliance, he/she is being allowed to see the classified Order in its entirety despite the fact that he/she does not have a security clearance and, presumably, does not have a proper storage facility. With that background, the agent should provide a security briefing that spells out the obligations and responsibilities of the custodian that arise out of the receipt of classified information. Chief among these is the obligation not to engage in unauthorized disclosure of classified information. During the security briefing, the custodian must be informed of the consequences of such unauthorized disclosure, which are the criminal penalties set forth in Title 18 of the United States Code, Sections 793 and 794.⁹ More specifically, per the FISC Order, the custodian must be advised that he/she may not disclose to any other person other than those persons necessary to produce the business records sought under the Order, that the FBI has sought or obtained these business records under the Order. Thus, the only authorized disclosure is disclosure of only such information and to only such persons as is necessary to produce the business records. Included in this category is disclosure of information sufficient to enable the custodian of records to consult with legal counsel for the purpose of determining the custodian's or entity's legal obligations under the Order.

Since the custodian of records presumably will be lacking not only a security clearance but also a facility to properly store the classified FISC order, the custodian must agree to the custodial trust procedures set forth herein. The

⁹ Section 793, "Gathering, transmitting or losing defense information," and Section 794, "Gathering or delivering defense information to aid foreign government," prohibit the unauthorized disclosure of national security information and provide for penalties from ten years (section 793) to life in prison or death (Section 794).

To: Counterterrorism From: Office of the General Counsel
Re: 08/23/2005

b7E

custodian must agree that once having read the Order, he/she will not maintain possession of it but will return it to the FBI, where the custodian will be allowed to see it upon request. Upon advance notice to the FBI, legal counsel will also be permitted to see it if the FBI is able to perform the preliminary background check of the lawyer, as described above. The custodian of records may take notes based on a reading of the Order but those notes may not reflect any information other than the subject's name, identifiers, and/or account number, and the nature of the information sought. The custodian of records may then keep those notes until he/she produces the business records, at which time, the custodian must turn the notes over to the FBI.

Once the custodian of records has been informed of these procedures and has agreed to them, he/she should be permitted to read the Order in its entirety, and take such notes as are described above.

The final step is for the custodian and the serving agent to sign the enclosed Model Custodial Trust Receipt. The first part of the Model Custodial Trust Receipt form is an acknowledgment by the FBI that the custodian of records has been given authorized access to a classified order; that the FBI will maintain custody and control of the Order and that the custodian of records and/or his/her legal representative will have access to the Order if necessary for compliance; and that the custodian of records may take notes under certain conditions, as set forth above, but must turn the notes over to the FBI when the business records are produced. The second part of the Model Custodial Trust Receipt acknowledges the custodian's understanding of the receipt procedures, as well as an agreement to comply with the specific non-disclosure terms set out in the business records order. It also informs the custodian of the criminal penalties under 18 U.S.C. §§ 793 and 794, that attach to unauthorized disclosure of sensitive national security information.¹⁰

When the Model Custodial Trust Receipt has been signed, the form should be retained by the FBI, with a copy provided to the custodian of records.¹¹

¹⁰ Since the Model Custodial Trust Receipt has been revised to fit this particular situation, there is no need for the custodian to sign an SF 312 form.

¹¹ The best practice is to have two copies of the form available for signature so that both the custodian of records and the FBI may have a signed copy.

To: Counterterrorism From: Office of the General Counsel
Re: [REDACTED] 08/23/2005

b7E

Upon production of the business records to the FBI, the agent must make sure that the custodian of records has turned over any written notes that he/she may have taken.

Upon service of the Order, the serving agent should fill out a Certificate of Service to document the service. A model certificate of service is attached and it or a variation may be used. The agent should retain the original of the signed certificate and provide a copy to the custodian of records, as it sets out the point of contact (which should be an agent at the field office where the Order will be held in trust). If possible, the copy should also be signed by the agent, or at least be dated, in order to provide a record for the custodian as to the date from which the time to comply set forth in the Order starts to run.¹²

Conclusion:

Any questions about the business records process should be addressed to the Office of the General Counsel, Assistant General Counsel [REDACTED]

b6
b7C

LEAD(s) :

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

¹² The best practice is to have two copies of this document available for signature so that both the custodian of records and the FBI may have a signed copy.

To: Counterterrorism From: Office of the General Counsel
Re: [redacted] 08/23/2005

b7E

Distribute to all supervisory personnel involved in the investigation of counterintelligence, counterterrorism, and cyber cases.

1 - Ms. Caproni

1 - [redacted]
1 - [redacted]
1 - [redacted]

b6
b7C

◆◆

U.S. Department of Justice
Office of the Inspector General

DATE: 03-22-2012
FBI INFO.
CLASSIFIED BY 65179 DMH/STP/MJS
REASON: 1.4 (c)

~~SECRET~~

A Review of the FBI's Use of Section 215 Orders for Business Records in 2006 (U)



Office of the Inspector General
March 2008

~~SECRET~~

DRV FROM: Federal Bureau of Investigation
Classification: 63675 UC/CTLU II/NSLB
Dated: March 10, 2008
DECL ON: March 10, 2033

ACLU Sect. 215-1467

TABLE OF CONTENTS (U)

TABLE OF CONTENTS (U).....i

INDEX OF CHARTS AND TABLES (U).....v

CHAPTER ONE: INTRODUCTION (U).....1

I. The Patriot Act and the Patriot Reauthorization Act of 2005 (U)2

II. Methodology of the OIG Review (U)2

III. Organization of the Report (U)3

IV. Summary of OIG Findings (U).....4

CHAPTER TWO: BACKGROUND (U).....7

I. Introduction (U).....7

II. Legal Background (U)7

III. The Process for Seeking Section 215 Orders (U)10

IV. How Section 215 Information is Collected, Analyzed, Retained, and Disseminated (U)11

CHAPTER THREE: OVERVIEW OF SECTION 215 REQUESTS PROCESSED IN 2006 (U).....13

I. Introduction (U).....13

II. Two Uses of Section 215 Authority (U)14

A. Pure Section 215 Applications (U)14

1. Number of Pure Section 215 Applications (U)15

2. Subjects of Pure Section 215 Applications (U)16

3. Types of Records Requested in Section 215 Applications (U)18

4. FBI Field Offices that Submitted Requests for Section 215 Applications (U)19

5. Types of Investigations from which Section 215 Requests Originated (U)20

B. Combination Section 215 Applications and Orders in 2006 (U).....20

ACLU Sect. 215-1468

- 1. Number of Combination Applications Submitted to and Approved by the FISA Court (U)21
- 2. Types of Records Requested in Combination Orders (U).....21
- 3. Number of U.S. Persons Identified as Subjects in Combination Orders (U).....21
- 4. FBI Field Offices that Initiated Requests for Combination Orders (U).....22
- 5. Types of Investigations from which Combination Orders Originate (U).....22

CHAPTER FOUR: SECTION 215 REQUESTS PROCESSED IN 2006 (U) ...23

I. Pure Section 215 Requests (U).....23

A. Requests for which Section 215 Orders Were Obtained (U)23

- 1. Request for [redacted] 23
- 2. Request for [redacted] 24
- 3. Request for [redacted] 25
- 4. Request for [redacted] 26
- 5. Request for [redacted] 27
- 6. Request for [redacted] 29
- 7. Request for [redacted] 29
- 8. Request for [redacted] 30
- 9. and 10. Requests for [redacted] 31
- 11. Request for [redacted] 32

B. Section 215 Requests that were Withdrawn (U)33

- 1. Request for [redacted] ...33
- 2. Request for [redacted] ...34
- 3. Request for [redacted] ...35
- 4. Request for [redacted] ...35
- 5. Request for [redacted] ...36
- 6. Request for [redacted] ...36

II. Combination Section 215 Requests (U)36

A. Use of Combination Orders (U).....36

B. Modifications and Notations to Combination Orders (U).....38

CHAPTER FIVE: OIG ANALYSIS (U).....39

I. Delays in Implementing Section 215 Authority and Other Impediments to Use (U)39

b1

(S)

(S)

- A. Pure Section 215 Processing Times in 2006 (U)39
- B. Pure Section 215 Processing Times 2004-2006 (U)43
- C. Bureaucratic and Procedural Impediments (U)45
 - 1. FBI Employees' Unfamiliarity with Section 215 Requests and the Approval Process (U)45
 - 2. OIPR Resources (U).....47
 - 3. Multi-Layered Review Process (U).....47
- D. Substantive Delays (U)48
 - 1. Nature of the Record (U)48
 - 2. The Statutory Requirements (U).....48
- E. Expedited Requests (U)50
- F. Unremarkable Applications (U).....50
- II. Modified Pure and Combination Section 215 Orders (U).....50
 - A. Handwritten Modifications (U).....51
 - B. Revised Applications and Orders (U).....51
- III. Use and Effectiveness of Information Obtained from Section 215 Orders (U)52
 - A. Use in Investigations (U).....52
 - (S) 1. [Redacted]53
 - 2. Support Additional Investigative Requests (U)53
 - 3. Investigate Leads (U).....53
 - B. Dissemination (U)54
 - C. Use in Criminal Proceedings (U)54
- IV. Effectiveness of Section 215 (U)55
 - A. Use of Section 215 Orders (U).....55
 - 1. Other Investigative Options (U)55
 - 2. Effect of the Processing Delays (U)56
 - B. Value of Section 215 Orders (U).....57
- V. Summary (U).....57
- CHAPTER SIX: IMPROPER OR ILLEGAL USE OF SECTION 215 AUTHORITY AND OTHER NOTEWORTHY FACTS (U)59
 - I. Two Instances in which the FBI Received More Information than it had Requested in Response to a Section 215 Order (U)59
 - A. Case 1 (U)60

b1

B. Case 2 (U)62

II. Other Noteworthy Items (U)65

(S) A. Request for [redacted]65

 1. The FBI Investigation (U).....65

 2. The FISA Court's Objections to the Section 215
Application on First Amendment Grounds (U)68

 3. FBI and OIPR's Response (U)70

 4. OIG Analysis (U)73

(S) B. [redacted] of Some Section 215 Requests ~~(S)~~74

CHAPTER SEVEN: MINIMIZATION PROCEDURES (U)75

I. Minimization Mandate (U).....75

II. Draft Minimization Procedures (U).....76

III. The Interim Standard Minimization Procedures (U).....79

IV. OIG ANALYSIS (U)81

CHAPTER EIGHT: CONCLUSIONS (U).....84

UNCLASSIFIED APPENDIX (U)

CLASSIFIED APPENDICES 1 and 2 (U)

b1

INDEX OF CHARTS AND TABLES (U)

	<u>Page</u>
CHART 5.1 Processing Time for 11 "Pure" Section 215 Requests Processed in 2006 (U)	41
CHART 5.2 Processing Time for Six Withdrawn "Pure" Section 215 Requests Processed in 2006 (U)	42
CHART 5.3 FBI Headquarters and OIPR Average Processing Time for Section 215 Requests from 2004 through 2006 (U)	44
CHART 5.4 FBI Headquarters and OIPR Average Processing Time for Section 215 Orders from 2004 through 2006 (U)	45
TABLE 3.1 Pure Section 215 Applications Processed by NSLB or OIPR in 2006 (U)	15
TABLE 3.2 Pure Section 215 Orders Issued by the Foreign Intelligence Surveillance Court (U)	16
TABLE 3.3 Number of U.S. Persons and Non-U.S. Persons Identified as Subjects in Section 215 Applications Processed in 2006 (U)	16
TABLE 3.4 Number of U.S. Persons and Non-U.S. Persons Identified as Subjects in Section 215 Orders Processed from 2002 through 2006 (U)	17
TABLE 3.5 Types of Records Requested in Pure Section 215 Applications Processed in 2006 and Approved by the FISA Court (U)	18
TABLE 3.6 Types of Records Requested in Pure Section 215 Applications Processed in 2006 and Withdrawn (U)	18
TABLE 3.7 Types of Records Requested in Pure Section 215 Orders between 2002 and 2006 and Approved by the FISA Court (U)	19
TABLE 3.8 Types of Investigations that Generated Pure Section 215 Requests Processed in 2006 and Approved by the FISA Court (U)	20

~~SECRET~~

CHAPTER ONE INTRODUCTION (U)

The *USA PATRIOT Improvement and Reauthorization Act of 2005* (Reauthorization Act or the Act) directed the Department of Justice (Department or DOJ) Office of the Inspector General (OIG) to conduct "a comprehensive audit of the effectiveness and use, including improper or illegal use" of the Federal Bureau of Investigation's (FBI) investigative authority that was expanded by Section 215 of the Patriot Act.¹ See Pub. L. No. 109-177, § 106A. Section 215 of the Patriot Act allows the FBI to seek orders from the Foreign Intelligence Surveillance Court (FISA Court) for "any tangible things," including books, records, and other items from any business, organization, or entity provided the item or items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities. The Reauthorization Act also required the OIG to review the FBI's use of Section 215 for two time periods - calendar years 2002 through 2004 and 2005 through 2006.² (U)

On March 9, 2007, the OIG issued our first report, which reviewed the use of Section 215 in 2002 through 2005.³ This is the OIG's second report required by the Reauthorization Act. This report examines the FBI's requests for Section 215 orders in 2006. In addition, as required by the Reauthorization Act, this report examines the minimization procedures for business records which the Reauthorization Act required the Attorney General to adopt in 2006. (U)

* This report includes information that the Department of Justice considered to be classified and therefore could not be publicly released. To create the public version of the report, the OIG redacted (deleted) the portions of the report that the Department considered to be classified, and we indicated where those redactions were made. In addition, the OIG has provided copies of the full classified report to the Department, the Director of National Intelligence, and Congress. (U)

¹ The term "USA PATRIOT Act" is an acronym for the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001). It is commonly referred to as "the Patriot Act." (U)

² The *USA PATRIOT Improvement and Reauthorization Act of 2005* (Reauthorization Act or the Act) also directed the OIG to conduct reviews on the use and effectiveness of the FBI's use of national security letters (NSL), another investigative authority that was expanded by the Patriot Act. The OIG reviews of the FBI's use of NSL authority are contained in separate reports. The OIG's first report on NSLs, issued in March 2007, reviewed the FBI's use of NSLs in 2003 through 2005. The OIG is issuing a second report on NSLs that examines the FBI's and Department's corrective actions taken in response to our first NSL report and the FBI's use of NSLs in 2006. In addition, the OIG is completing a third report on the FBI's use of "exigent letters." (U)

³ Although we were only required to review 2002 through 2004 in the first review, we elected to include data from 2005 in that report. (U) ACLU Sect. 215-1473

1
~~SECRET~~

I. The Patriot Act and the Patriot Reauthorization Act of 2005 (U)

Enacted after the September 11, 2001, terrorist attacks, the Patriot Act states that it seeks to provide federal authorities "with the appropriate tools required to intercept and obstruct terrorism." Several Patriot Act provisions, including Section 215, were originally scheduled to sunset on December 31, 2005. On March 9, 2006, the President signed into law the Reauthorization Act, which, among other things, made permanent or extended several Patriot Act provisions. However, Section 215 was not made permanent but was extended for 4 years until December 31, 2009. The Reauthorization Act also resulted in several substantive changes to Section 215, which we discuss in Chapter Two of this report. (U)

II. Methodology of the OIG Review (U)

In this review of the use of Section 215 orders, the OIG examined documents obtained from the FBI and the Department's Office of Intelligence Policy and Review (OIPR) relating to each instance of the FBI's use or attempted use of Section 215 authorities during 2006.⁴ In addition, we reviewed Department reports concerning the FBI's use of Section 215 authorities. (U)

In this review, the OIG conducted over 60 interviews of FBI, Department, and other officials. The OIG also visited FBI field offices in New York City and suburban Maryland to review investigative case files from which requests for Section 215 applications originated and to interview FBI employees, including FBI Special Agents in Charge (SAC), Assistant Special Agents in Charge, Chief Division Counsels, Supervisory Special Agents, case agents, and intelligence analysts.⁵ We also conducted telephone interviews of FBI employees in several other field offices who had initiated Section 215 requests. (U)

The OIG also interviewed senior FBI and OIPR officials who participated in implementing procedures and processing requests for Section 215 orders, including OIPR's former Acting Counsel and former Counsel for Intelligence Policy, the FBI General Counsel and the Deputy

⁴ Until fall 2006, the Office of Intelligence Policy Review (OIPR) was a separate component of the Department. In March 2006, the Reauthorization Act authorized the creation of a National Security Division (NSD) within the Department. In September 2006, Kenneth L. Wainstein was confirmed as the first Assistant Attorney General for the NSD, and shortly after that OIPR was moved to the NSD. OIPR's and NSD's intelligence functions will be reorganized within NSD's planned Office of Intelligence. Because the reorganization is not yet complete, we refer to OIPR in this report. (U)

⁵ FBI field offices are also referred to as "divisions." The Chief Division Counsel is the chief legal officer for the field office. (U)

General Counsel of the FBI Office of General Counsel's National Security Law Branch (NSLB), other attorneys and personnel from NSLB and OIPR, and officials responsible for administering the FBI and OIPR Section 215 tracking systems. (U)

III. Organization of the Report (U)

This report is divided into eight chapters followed by one unclassified appendix and two classified appendices. After this introduction, we describe in Chapter Two the legal background related to Section 215 authority and the processes for seeking Section 215 orders and for retaining and disseminating records received pursuant to those orders. (U)

In Chapter Three, we provide an overview of the instances in which the FBI sought to obtain Section 215 orders in 2006, including the number of FBI requests, the number of orders obtained, and the type of information requested. (U)

In Chapter Four, we provide a detailed description of the FBI's requests for Section 215 orders processed in 2006. We describe the records requested; the purpose of the requests; the processing time for the requests; whether the applications were granted, modified, or withdrawn; whether the records were produced; and if so, how they were used. (U)

In Chapter Five, we present our findings and analysis of the 2006 applications and orders, including their processing time, Foreign Intelligence Surveillance Court modifications, and their use and effectiveness. (U)

In Chapter Six, we identify any improper, illegal, or noteworthy use of Section 215, and in Chapter Seven we examine the minimization procedures adopted by the Attorney General in response to the Reauthorization Act. (U)

Chapter Eight contains our conclusions. (U)

The Unclassified Appendix to the report contains the comments on the report by the Director of National Intelligence, the Assistant Attorney General for the National Security Division, and the Director of the FBI. (U)

The two Classified Appendices describe other uses of Section 215 (S) orders to collect

b1

IV. Summary of OIG Findings (U)

Our review determined that, similar to the findings of our first report on Section 215 orders, the FBI and OIPR processed various FBI requests for the use of both "pure" and "combination" Section 215 orders in 2006.⁶ In 2006, the FBI and OIPR processed 15 pure Section 215 applications and 32 combination applications which were formally submitted to the FISA Court. All 47 Section 215 applications submitted to the FISA Court were approved.⁷ The Section 215 applications requested a variety of information, including credit card records, [redacted]

b1

Unlike in previous years, [redacted]

We also determined that during the period covered by this report FBI agents encountered similar processing delays for Section 215 applications as those identified in our previous report. These delays were caused by unfamiliarity with the Section 215 process, too few resources to handle requests expeditiously, a multi-layered review process, and various substantive issues regarding whether certain applications met the statutory requirements. Overall, the average processing time for Section 215 orders in 2006 was 147 days, which was similar to the processing times for 2005. However, the FBI and OIPR were able to expedite certain Section 215 requests in 2006, and when the FBI identified two emergency requests the FBI and OIPR processed both Section 215 requests quickly. (U)

Similar to our previous report, we examined how the FBI has used information obtained from Section 215 orders in national security investigations. Aside from [redacted] [redacted] we found that in 2006 Section 215 orders were used primarily to exhaust investigative leads, although in some instances the FBI obtained information to support additional FBI investigative requests and to [redacted]

⁶ Pure Section 215 requests are not associated with applications for the use of any other *Foreign Intelligence Surveillance Act* (FISA) authority. Combination Section 215 requests are business record requests added to or combined with a FISA application for pen register/trap and trace orders. (U)

⁷ Four of the pure Section 215 applications processed in 2006 were signed by the FISA Court in 2007. (U)

~~SECRET~~

We did not identify any illegal use of Section 215 authority. However, our review identified two instances in which the provider produced records that were in response to, but outside the scope of, Section 215 orders. In one of these two instances, the FBI quickly determined that it had inadvertently received information not authorized by the Section 215 orders and took appropriate steps to address the matter. In the other case, approximately 2 months passed before the FBI recognized and addressed the matter. As a result, we recommend that the FBI develop and implement procedures to ensure that FBI employees check that they are not receiving or using information that is not authorized by the Section 215 order. (U)

Our review also identified that the FBI reported only one of the two matters to the President's Intelligence Oversight Board (IOB).⁸ The FBI determined that only one of the two instances involved statutorily protected material and that only the instance involving the statutorily protected material was reportable to the IOB. The FBI also determined that the non-statutorily protected material should be considered as voluntarily produced material even though the provider had refused to produce the material without a court order. (U)

As a result, we recommend that the FBI develop procedures for identifying and handling material that is produced in response to, but outside the scope of, Section 215 orders. The procedures should include the FBI's justification for handling any class of such material differently from other classes. We believe the FBI should not base the procedures for handling such material solely on whether the material is or is not statutorily protected. For example, the procedures should address additional factors such as whether the material contains non-public information about U.S. persons who are not the subjects of FBI national security investigations, and whether the underlying Section 215 order included particularized minimization procedures. (U)

(S) We also identified two other "noteworthy" issues. First, we found that the FBI had issued national security letters (NSL) for information about [redacted] [redacted] after the FISA Court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation. We questioned the appropriateness of the FBI's issuing these NSLs after the Court's decision because NSLs have the same First Amendment caveat as Section 215 requests and the FBI issued the NSLs based on the same factual predicate, without further reviewing the underlying investigation to ensure that it was not premised solely on protected First Amendment conduct. ~~(S)~~

b1

⁸ In 1976 the Intelligence Oversight Board (IOB) was created by Executive Order and charged with reviewing activities of the U.S. intelligence community and informing the President of any activities that the IOB believes "may be unlawful or contrary to executive order or Presidential Directives." See Executive Order 12863. (U)

5
~~SECRET~~

ACLU Sect. 215-1477

(S) The second noteworthy issue

b1



Finally, as directed by the Reauthorization Act, we also examined whether the interim minimization procedures adopted by the Department for Section 215 orders protect the constitutional rights of U.S. persons. We concluded that the standard minimization procedures adopted in September 2006, which are interim procedures, do not adequately address the intent and minimization requirements of the Reauthorization Act, and we recommend that the Department develop specific standard minimization procedures relating to Section 215 orders. (U)

CHAPTER TWO BACKGROUND (U)

I. Introduction (U)

This chapter provides a brief description of the legal background related to Section 215 authority and the process for obtaining Section 215 orders. (U)

II. Legal Background (U)

Pursuant to Section 215 of the Patriot Act, the FBI may obtain "any tangible things," including books, records, and other items from any business, organization, or entity provided that the item or items are for an authorized investigation. The tangible things are available "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 an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. § 1861. Section 215 did not create any new investigative authority but instead expanded existing authority found in the *Foreign Intelligence Surveillance Act of 1978* (FISA). 50 U.S.C. § 1801 et seq. (U)

FISA requires the FBI to obtain an order from the Foreign Intelligence Surveillance Court (FISA Court) in order to conduct electronic surveillance to collect foreign intelligence information.⁹ In 1998, Congress amended FISA to authorize the FBI to apply to the FISA Court for orders compelling four kinds of businesses to "release records in its possession" to the FBI: common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. The amendment did not further define "records." This provision, which was codified at 50 U.S.C. § 1862, became known as the "business records" provision and was the provision expanded by Section 215 of the Patriot Act.¹⁰ (U)

The 1998 business records amendment required a FISA application to specify that the records were sought for an investigation to gather foreign intelligence information or an investigation concerning international

⁹ OIPR prepares and presents applications for Section 215 orders to the FISA Court on behalf of the FBI. According to the FISA Court Rules of Procedures, the Attorney General determines who is permitted to appear before the FISA Court, and FBI attorneys have not been authorized to appear before the Court for this purpose. (U)

¹⁰ 50 U.S.C. § 1862(b)(2)(B) (1998), as amended, 50 U.S.C. § 1861 (2001). (U)

~~SECRET~~

terrorism, and that there were "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." 50 U.S.C. § 1862 (2000 ed.). This language meant that the FBI was limited to obtaining information regarding a specific person or entity the FBI was investigating and about whom the FBI had individualized suspicion. In addition, the amendment prohibited the entity complying with the order from disclosing either the existence of the order or any information produced in response to the order. (U)

Subsequent to the 1998 FISA amendment creating this investigative authority and prior to passage of the Patriot Act in October 2001, the FBI obtained only one FISA order for business records. This order was obtained in 2000. (U)

Section 215 of the Patriot Act significantly expanded the scope of the FBI's investigative authority pursuant to the business records provision of FISA and lowered the standard of proof required to obtain this type of business record. The pertinent part of Section 215 provides: (U)

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.¹¹ 50 U.S.C. § 1861(a)(1).
(U)

While the 1998 language limited the reach of this type of investigative authority to four types of entities, the new language did not explicitly limit the type of entity or business that can be compelled by an order. Section 215 of the Patriot Act also expanded the categories of documents that the FBI can obtain under the business records provision of FISA, because it no longer was limited to "records" and provides that the FBI may obtain an order for "the production of any tangible things (including books, records, papers, documents, and other items)." *Id.* (U)

¹¹ "United States person" is defined as a citizen, legal permanent resident, an unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, or corporations incorporated in the United States as long as such associations or corporations are not themselves "foreign powers." 50 U.S.C. § 1801(i).
(U)

ACLU Sect. 215-1480

8
~~SECRET~~

Section 215 also lowered the evidentiary threshold to obtain such an order. As a result, the number of people whose information could be obtained was expanded because the FBI is no longer required to show that the items being sought pertain to a person whom the FBI is investigating. Instead, the items sought need only be requested "for an authorized investigation conducted in accordance with [applicable law and guidelines] 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). This standard, referred to as the relevance standard, permits the FBI to seek information concerning persons not necessarily under investigation but who are connected in some way to a person or entity under investigation. (U)

The Reauthorization Act further amended Section 215 by requiring that an application establish "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." *Id.* At the same time, the Reauthorization Act provided for a presumption of relevance for four specified entities or individuals: foreign powers, agents of foreign powers, subjects of authorized counterterrorism or counterintelligence investigations, and individuals known to associate with subjects of such investigations. *Id.* When an application involves one of the four entities or individuals referenced in the presumption, the applicant need not establish reasonable grounds to believe the requested items are relevant. (U)

The Reauthorization Act included other substantive amendments to Section 215. For example, the Act specifically authorized the collection of certain sensitive records, including library, medical, educational, and tax return records. The Act also required that an application for these sensitive records be approved by the FBI Director or a specified designee, and specific congressional reporting.¹² In addition, the Reauthorization Act specifically provided that Section 215 orders must, among other things, contain a particularized description of the items sought and provide for a reasonable time to assemble them. The Act also established a detailed judicial review process for recipients of Section 215 orders to challenge their legality before a FISA Court judge and extended Section 215 for 4 years until December 31, 2009. (U)

Additional changes to Section 215 were adopted with the enactment of the *USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006*. For example, the 2006 amendments provided that a recipient of a Section 215 order may petition the FISA Court to modify or set aside the nondisclosure

¹² As permitted by the Reauthorization Act, the FBI Director delegated approval authority for these records to the Deputy Director and the Executive Assistant Director for the FBI's National Security Branch. (U)

~~SECRET~~

requirement after 1 year from the issuance of the order if certain findings are made.¹³ (U)

III. The Process for Seeking Section 215 Orders (U)

As we described in our March 2007 report regarding the use of Section 215 orders from 2002 through 2005, the process to obtain a Section 215 order generally involves five phases: FBI field office initiation and review, FBI Headquarters review, OIPR review, FISA Court review, and FBI service of the order. (U)

The process to obtain a Section 215 order normally begins when an FBI case agent in a field office prepares a business records request form, which requires the agent to provide, among other things, the following information: a brief summary of the investigation, a specific description of the items requested, an explanation of the manner in which the requested items are expected to provide foreign intelligence information, and the identity of the custodian or owner of the requested items. The request form must be approved by the squad's Supervisory Special Agent, the Chief Division Counsel, and the SAC at the FBI field office. The approval process is automated through the FBI's FISA Management System (FISAMS), which sends electronic notifications to each individual responsible for taking the next action in order to process the business record in the field office. After the approvals are completed in the field office, the FISAMS notifies the "substantive desk" (in the Counterterrorism Division or Counterintelligence Division) at FBI Headquarters. (U)

At FBI Headquarters, the business records request form is reviewed and approved by both the substantive desk and the Office of General Counsel's NSLB. Once the FISAMS delivers the request to the substantive desk, it is assigned to an NSLB attorney who works with the case agent and other FBI personnel to obtain the information the NSLB attorney believes is necessary to include in the draft application and order. The draft application package is then reviewed by NSLB supervisors and forwarded to OIPR, where the request is assigned to an OIPR attorney. (U)

¹³ USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178. The Court may grant a petition to modify or set aside a petition if the Court finds there is no reason to believe that disclosure may endanger the national security, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety any person. However, if the Attorney General, Deputy Attorney General, or FBI Director certifies that the disclosure may endanger the national security or interfere with diplomatic relations, the certification will be treated as conclusive unless the Court finds that such a certification was made in bad faith. (U)

ACLU Sect. 215-1482

~~10
SECRET~~

~~SECRET~~

The OIPR attorney works with the NSLB attorney, case agents, and occasionally FBI intelligence analysts to obtain the information the OIPR attorney believes is necessary to include in the draft application and order. An OIPR supervisor then reviews the draft application package. The final application package is returned to the FBI for an accuracy review and additional edits may be made based on the FBI's review of the final package. Upon completion of the final version, signatures of designated senior FBI personnel are obtained and an OIPR attorney prepares the package for presentation to the FISA Court. (U)

While the final signatures are collected, OIPR schedules the case on the FISA Court's docket for a hearing and provides the FISA Court with an advance copy of the application and order, which is called a "read" copy. The FISA Court, through a FISA Court legal advisor, may identify concerns and request changes to the documents after reviewing the "read" copy. OIPR and the FBI then address the Court's questions or concerns and make revisions to the application or order. If the FISA Court deems it necessary, OIPR then formally presents the application package to the FISA Court at the scheduled hearing.¹⁴ If the FISA Court judge approves the application, the judge signs the order. At the hearing, the judge may make handwritten changes to the order and, if so, will sign the order with the handwritten modifications. (U)

The order is then entered into the FISAMS and served by the FBI field office nearest to the provider designated in the order. Among other things, the order sets forth the time period for producing the items. (U)

IV. How Section 215 Information is Collected, Analyzed, Retained, and Disseminated (U)

The FBI continues to collect, analyze, and retain Section 215 information as described in our previous report. In brief, a Section 215 order is served by the FBI office nearest the custodian of records named in the Court order. The records are either provided to the FBI in hard copy or in electronic format. Upon receipt, the records may be uploaded into the Automated Case Support (ACS) system, the FBI's electronic case file system, or reviewed and analyzed by the case agent or an FBI analyst. If the records are provided in electronic format, they may be uploaded into the ACS system by a technician prior to an agent's review. If the records are provided in paper format, the agent may review them and if the case agent determines no further investigation is warranted, the agent may store the information with the rest of the investigative case file. Whether provided in paper or electronic format, the case agent may write an Electronic

(S)

b1

~~11
SECRET~~

ACLU Sect. 215-1483

~~SECRET~~

Communication (EC) summarizing the information obtained for purposes of documenting the existence of the records electronically in the ACS system.
(U)

If the information warrants dissemination within the FBI, the agent prepares an EC to the relevant field office or offices. If the information warrants dissemination outside of the FBI, [redacted]

(S) [redacted] the agent provides the records to the appropriate FBI office for approval. [redacted]

b1

ACLU Sect. 215-1484

~~12
SECRET~~

**CHAPTER THREE
OVERVIEW OF SECTION 215 REQUESTS
PROCESSED IN 2006 (U)**

I. Introduction (U)

As part of the OIG's review of the use and effectiveness of Section 215 authorities, the Reauthorization Act directed the OIG to examine the following: (U)

- Every business record application submitted to the FISA Court including whether: (a) the FBI requested that the Department of Justice submit a business record application to the FISA Court and the application was not submitted, and (b) whether the FISA Court granted, modified, or denied any business record application; (U)
- Whether bureaucratic or procedural impediments prevented the FBI from "taking full advantage" of the FISA business record provisions; (U)
- Any noteworthy facts or circumstances concerning the business record requests, including any illegal or improper use of the authority; (U)
- The effectiveness of the business record requests as an "investigative tool," including: (a) what types of records are obtained and the importance of those records in the intelligence activities of the FBI and the DOJ; (b) the manner in which the information obtained through business record requests is collected, retained, analyzed, and disseminated by the FBI; (c) whether and how often the FBI used information obtained from business record requests to produce an "analytical intelligence product" for distribution to, among others, the intelligence community or federal, state, and local governments; and (d) whether and how often the FBI provided information obtained from business record requests to law enforcement authorities for use in criminal proceedings; and (U)
- With respect to 2006, an examination of the minimization procedures adopted by the Attorney General pursuant to the Reauthorization Act and whether such minimization procedures protect the constitutional rights of United States persons.¹⁵ (U)

¹⁵ The Reauthorization Act also directed that the OIG examine the justification for the failure of the Attorney General to issue implementing procedures governing requests for (Cont'd.).

In this chapter we provide an overview of FBI requests for Section 215 orders that were processed in 2006. We describe the number of requests submitted by FBI agents, the number of Section 215 orders obtained, the type of information requested, and the number of requests that were withdrawn. (U)

II. Two Uses of Section 215 Authority (U)

In 2006, as in previous years, FBI Headquarters and OIPR submitted to the FISA Court applications for two different kinds of Section 215 authority: "pure" and "combination" Section 215 applications. (U)

A "pure" Section 215 application is a term used by OIPR to refer to a Section 215 application for any tangible item that is not associated with applications for any other FISA authority. For example, a Section 215 request for driver's license records from state departments of motor vehicles would constitute a pure Section 215 request. (U)

A "combination" application is a term used by OIPR to refer to a Section 215 request that is added to or combined with a FISA application for pen register/trap and trace orders.¹⁶ The use of the combination request evolved from OIPR's determination that FISA pen register/trap and trace orders did not require providers to turn over subscriber information associated with telephone numbers obtained through the orders.¹⁷ (U)

A. Pure Section 215 Applications (U)

We reviewed all pure Section 215 applications that NSLB or OIPR processed in 2006 for submission to the FISA Court. In this section, we describe the number of pure Section 215 requests; the number of pure applications formally submitted to and approved by the FISA Court; the number of U.S. and non-U.S. persons that were the subjects of these applications; the types of records obtained; the FBI field offices that requested Section 215 applications; and the types of investigations that generated Section 215 requests. (U)

business records applications and whether such delay harmed national security. We addressed this request in our March 2007 Section 215 report. (U)

¹⁶ A pen register is a surveillance device that captures the phone numbers dialed on outgoing telephone calls; trap and trace devices capture the numbers identifying incoming calls. (U)

¹⁷ We discuss the origin of combination requests in more detail in Chapter Three of our March 2007 report. (U)

1. Number of Pure Section 215 Applications (U)

In 2006, the FBI or OIPR processed 21 requests for pure Section 215 applications. Of these, 15 were formally submitted to the FISA Court for approval - 11 were submitted in 2006 and 4 were submitted in 2007.¹⁸ The six additional requests were "withdrawn." Withdrawn applications are those which are either not presented or not formally presented to the FISA Court for approval.¹⁹ (U)

Each of the 15 formal submissions processed in 2006 was approved by the FISA Court. Table 3.1 illustrates this information. (U)

(S)



b1

**TABLE 3.1
Pure Section 215 Applications
Processed by NSLB or OIPR in 2006 (U)**

	2006*(U)
Number of applications processed during 2006 and formally submitted to the FISA Court (U)	15 (U)
Number of applications processed during 2006 and withdrawn (U)	6 (U)
Total applications processed during 2006 (U)	21 (U)

Source: OIPR and FBI (U)

*Note: The 15 applications processed during 2006 include 4 that the FISA Court approved in 2007. The six withdrawn applications processed during 2006 include one that was withdrawn in 2007. (U)

In total, between 2002 and 2006, 36 Section 215 applications were processed and formally submitted to the FISA Court. Each of the 36 was approved, as indicated in Table 3.2. (U)

¹⁸ OIPR formally submitted interim standard minimization procedures to the FISA Court in 2006. Although this submission was given a business record docket number, it was not a Section 215 application and therefore we do not count it as a business record application. We discuss the interim standard minimization procedures in Chapter Seven of this report. (U)

¹⁹ One of the six withdrawn applications was presented to the FISA Court twice as a "read" copy before it was withdrawn. We discuss the reasons for the withdrawn applications in Chapter Four. (U)

TABLE 3.2
Pure Section 215 Orders Issued by the
Foreign Intelligence Surveillance Court (U)

	2002 (U)	2003 (U)	2004 (U)	2005 (U)	2006* (U)	Total (U)
Total number of applications submitted to and approved by the FISA Court (U)	0 (U)	0 (U)	7 (U)	14 (U)	15 (U)	36 (U)

Source: OIPR and FBI (U)

*Note: The 15 applications processed during 2006 include 4 that the FISA Court approved in 2007. (U)

2. Subjects of Pure Section 215 Applications (U)

We compiled the number of U.S. and non-U.S. persons who were identified as the subject of the Section 215 request and the underlying FBI investigation. We relied on the information provided in the Section 215 applications for this information.²⁰ Table 3.3 shows the results for applications processed in 2006. (U)

TABLE 3.3
Number of U.S. Persons and Non-U.S. Persons Identified as Subjects
in Section 215 Applications Processed in 2006* (U)

	Approved applications (U)	Withdrawn applications (U)	Total (U)
(S) U.S. Person (U)			
Non-U.S. Person (U)			

Source: OIPR and FBI (U)

*Note: Table 3.3 includes the four Section 215 orders processed in 2006 and signed in 2007 and excludes [redacted]

(S) The number of persons referenced in Table 3.3 is greater than the number of applications approved by the FISA Court because Section 215 applications can name more than one subject, and we counted each subject separately. [redacted] of the applications requested business records for more than one subject. [redacted] applications requested business records for [redacted] different subjects. ~~(S)~~

Moreover, Table 3.3 does not present the full universe of U.S. persons and non-U.S. persons named as subjects or otherwise affected by Section

²⁰ As previously stated, the FISA statute defines a "United States person" as a citizen, legal permanent resident, unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, or corporations incorporated in the United States as long as such associations or corporations are not themselves "foreign powers." 50 U.S.C. § 1801(i). (U) ACLU Sect. 215-1488

(S) 215 applications processed in 2006 for two reasons. First, Table 3.3 does not include individuals who were the subject of a Section 215 application but not the subject of an FBI investigation (a "non-subject"). We did not include the number of non-subjects because [redacted] Section 215 applications requested records of non-subjects, but [redacted] identified whether the non-subjects were U.S. or non-U.S. persons.²¹ (S)

b1

(S) Second, Table 3.3 does not reflect the number of U.S. persons and non-U.S. persons about whom information was collected as a result of [redacted]

(S) In our March 2007 report, we reported that in 2004 (the first calendar year in which pure applications were submitted to the FISA Court [redacted])

[redacted] With these important caveats, Table 3.4 shows the number of subjects that were identified as U.S. and non-U.S. persons for 32 of the 36 Section 215 applications processed from 2002 through 2006 and approved by the FISA Court. (S)

TABLE 3.4
Number of U.S. Persons and Non-U.S. Persons Identified as Subjects in Section 215 Orders Processed from 2002 through 2006 (U)

	2002 (U)	2003 (U)	2004 (U)	2005 (U)	2006* (U)	Total (U)
U.S. Person (U)	0 (U)	0 (U)				
Non-U.S. Person (U)	0 (U)	0 (U)				
Total	0 (U)	0 (U)				

Source: OIPR and FBI (U)

*Note: CY 2006 includes the four Section 215 orders processed in 2006 and signed in 2007 and excludes [redacted]

²¹ [redacted] Section 215 applications requested records for non-subjects. [redacted]

In total, 16 different types of records were requested in the Section 215 orders processed between 2002 and 2006 and approved by the FISA Court. The types of records are illustrated in Table 3.7. (U)

TABLE 3.7
Types of Records Requested in Pure Section 215 Orders
between 2002 and 2006 and Approved by the FISA Court* (U)

Type of Record Requested (U)	Approved Applications (U)
	Total

b1

(S)

Source: OIPR and FBI (U)

*Note: Table 3.7 includes the four Section 215 orders processed in 2006 and signed in 2007 and excluded [redacted]

(S)

4. FBI Field Offices that Submitted Requests for Section 215 Applications (U)

(S) The OIG also analyzed how many FBI field offices submitted requests for pure Section 215 applications. We determined that [redacted] of the FBI's 56 field offices ([redacted] percent) applied for the 17 pure Section 215 orders processed in 2006. A total of [redacted] FBI field offices ([redacted] percent) have requested Section 215 orders since 2002.²² (S)

²² As discussed in our first Section 215 report, there were no Section 215 orders approved in 2002 or 2003. The first Section 215 order was approved in May 2004. (U)

5. Types of Investigations from which Section 215 Requests Originated (U)

We also examined the types of investigations from which pure requests originated. The pure Section 215 applications originated from either counterintelligence (CI), counterterrorism (CT), or cyber investigations. Table 3.8 shows the types of investigations from which pure Section 215 applications processed in 2006 and approved by the FISA Court originated, excluding [redacted]

b1

TABLE 3.8

Types of Investigations that Generated Pure Section 215 Requests Processed in 2006 and Approved by the FISA Court (U)

Case Type (U)	2002 (U)	2003 (U)	2004 (U)	2005 (U)	2006 (U)	Totals (U)
CI (U)	0 (U)	0 (U)	3 (U)	6 (U)	4 (U)	13 (U)
CT (U)	0 (U)	0 (U)	4 (U)	4 (U)	6 (U)	14 (U)
Cyber (U)	0 (U)	0 (U)	0 (U)	1 (U)	1 (U)	2 (U)

Source: OIPR and FBI (U)

*Note: For 2006, Table 3.8 includes the four Section 215 orders processed in 2006 and signed in 2007 and excludes [redacted]

B. Combination Section 215 Applications and Orders in 2006 (U)

In this section, we describe the number and types of applications for combination orders that were submitted to the FISA Court in 2006. A combination application is a term used by OIPR to refer to a Section 215 request that was added to or combined with a FISA application for a pen register/trap and trace. The use of the combination request evolved from OIPR's determination that FISA pen register/trap and trace orders did not require providers to turn over subscriber information associated with telephone numbers obtained through those orders. As a result, Section 215 requests were added to pen register/trap and trace orders to seek subscriber information. OIPR also used combination orders in 2005 and 2006 to obtain [redacted]

After passage of the Reauthorization Act on March 9, 2006, combination orders became unnecessary for subscriber information and [redacted]

Section 128 of the Reauthorization Act amended the FISA statute to [redacted]

authorize subscriber information to be provided in response to a pen register/trap and trace order. Therefore, combination orders for subscriber information were no longer necessary. In addition, OIPR determined that substantive amendments to the statute undermined the legal basis for which OIPR had received authorization [redacted] from the FISA Court. Therefore, OIPR decided not to request [redacted] pursuant to Section 215 until it re-briefed the issue for the FISA Court.²⁴ As a result, in 2006 combination orders were submitted to the FISA Court only from January 1, 2006, through March 8, 2006. (S)

b1

1. Number of Combination Applications Submitted to and Approved by the FISA Court (U)

From January 1, 2006, through March 8, 2006, the FISA Court approved 32 combination business record applications. Of the 32 combination applications, 7 were new requests for combination orders and 25 were requests to renew or extend previous orders. (U)

2. Types of Records Requested in Combination Orders (U)

We determined that each business record application attached to the pen register/trap and trace applications included a request for subscriber information for the telephone numbers captured in the pen register/trap and trace. Some of the business record requests also included requests [redacted] [redacted] The 32 combination applications requested subscriber information [redacted] phone numbers. (S)

3. Number of U.S. Persons Identified as Subjects in Combination Orders (U)

As with the pure Section 215 orders, we identified the number of U.S. and non-U.S. persons identified as "subjects" in combination orders. We found that [redacted] subjects were named in the 32 combination orders. Of the subjects [redacted] were "U.S. persons" and [redacted] were "non-U.S. persons." (S)

²⁴ OIPR first briefed the issue to the FISA Court in February 2006, prior to the Reauthorization Act [redacted]

~~SECRET~~

**4. FBI Field Offices that Initiated Requests for
Combination Orders (U)**

b1

(S) We determined that FBI field offices submitted 32 combination applications approved by the FISA Court from January 1, 2006, through March 8, 2006. ~~(S)~~

**5. Types of Investigations from which Combination
Orders Originate (U)**

Of the 32 combination orders we reviewed, 25 were issued in counterterrorism cases and 7 were issued in counterintelligence cases. (U)

ACLU Sect. 215-1494

~~22~~
~~SECRET~~

CHAPTER FOUR
SECTION 215 REQUESTS PROCESSED IN 2006 (U)

In this chapter, we discuss the FBI's requests for Section 215 orders processed in 2006. We first describe pure section 215 requests and identify the types of records requested and any delays in the processing time.²⁵ If a Section 215 request was withdrawn, we identify the reasons for the withdrawal and at what stage it was withdrawn. If a Section 215 application and order was presented to the FISA Court, we identify whether the Court granted, modified or denied the request. If a Section 215 order was issued and records were received by the agent, we describe how the records were used. We then briefly discuss Section 215 combination orders. (U)

I. Pure Section 215 Requests (U)

In this section we discuss 11 of the 15 pure Section 215 requests processed in 2006 for which Section 215 orders were obtained and the 6 requests that were withdrawn. We do not discuss [redacted]

(S)

b1

A. Requests for which Section 215 Orders Were Obtained (U)

1. Request for [redacted]

(S)

An FBI agent submitted a Section 215 request for a [redacted] in a counterintelligence investigation.

(S)

The Section 215 request was processed in 188 days. [redacted]

(S)

²⁵ We do not discuss every delay in processing, only those which had a significant and identifiable effect on the overall processing time. (U)

ACLU Sect. 215-1495

(S)

[Redacted]

After reviewing the read application and order, the FISA Court requested that OIPR clarify the specialized minimization procedures and indicate that the specialized minimization procedures were in addition to the interim standard minimization procedures adopted by the Attorney General in September 2006. (U)

(S)

In response to the Section 215 order [Redacted]

[Redacted] The agent told the OIG that through this Section 215 request he learned that [Redacted]

(S)

[Redacted]

(S)

2. Request for [Redacted]

(S)

An FBI agent submitted a Section 215 request for [Redacted] in a counterintelligence investigation.

[Redacted]

(S)

[Redacted]

²⁶ Minimization procedures limit access, retention, and dissemination of business records. The Attorney General's interim standard minimization procedures applicable to all business records that were issued in September 2006 are discussed in Chapter Seven. (U)

This Section 215 request was processed in 175 days. The case was delayed initially for almost 2 months at the field office because the agent thought the request was pending at NSLB when it was actually awaiting approval by a field office supervisor. Once the request was drafted by NSLB and sent to OIPR, the two offices disagreed as to whether [redacted]

(S)

b1

[redacted]

According to the agent, the information received pursuant to the Section 215 order did not further the counterintelligence investigation. (U)

3. Request for [redacted]

(S)

An FBI agent submitted a Section 215 request in a counterintelligence investigation [redacted]

(S)

[redacted]

This request was processed in 203 days. [redacted]

(S)

[redacted]

[redacted] Ultimately, the FBI did neither. According to the FBI General Counsel, additional minimization procedures were not necessary because of the limited manner in which the FBI intended to use the information from this Section 215 request. ~~(S)~~

²⁷ A full FISA is a request for authority to conduct electronic surveillance or physical searches and is more detailed than a Section 215 request because the application must establish probable cause to believe, among other things, that the target is a foreign power or an agent of a foreign power. (U)

After reviewing the read application and order, the FISA Court requested that OIPR explain the relevance of an aspect of the request. According to OIPR e-mails, the OIPR attorney had previously asked NSLB the same question and was able to explain the relevance to the FISA Court. The court granted the Section 215 request. According to the case agent, the

(S) [redacted] produced an additional 2 months of records not authorized by the FISA Court order. (S)

b1

(S) The agent told the OIG that he made a copy of the [redacted] records that did not include the two additional months of [redacted] produced to the FBI but not authorized by the FISA Court order. The agent then sealed the [redacted] records that he had originally received from the provider into an envelope. (S)

(S) The agent stated that he sent the redacted copy of the records to FBI [redacted]. The agent stated that the additional records and the size [redacted] had delayed his evaluation of the portion of records appropriately produced pursuant to the Court order; however, he stated that he expected that these records would be useful. (S)

The FBI informed the OIG that it had determined that the receipt of additional records beyond the scope of the FISA Court order was not reportable to the Intelligence Oversight Review Board (IOB) and that the FBI would consider the additional material to be a voluntary production by the provider. OIPR had not yet decided whether the incident was reportable to the FISA Court.²⁸ (U)

(S) 4. Request for [redacted]
[redacted]

(S) An FBI agent submitted a Section 215 request in a counterintelligence investigation [redacted]

[redacted]

²⁸ We discuss this collection of additional records again in Chapter Six. (U)

(S) [Redacted]

This Section 215 request was processed in 120 days. The request raised questions concerning the appropriate use of a Section 215 order.

(S) [Redacted]

enforce the NSL with a court order. Instead, the NSLB attorney decided to request the records through a Section 215 application.

(S) [Redacted]

(S) As a result of the Section 215 order, [Redacted]

[Redacted]

(S) **5. Request for** [Redacted]

An FBI agent submitted a Section 215 request in a counterterrorism investigation

(S) [Redacted]

(S) [Redacted]

(S)

[Redacted]

(S)

This Section 215 request, processed in 125 days, raised 2 substantive issues. The first was a legal question as to whether [redacted] were business records within the meaning of Section 215 [redacted]

[redacted]

According to e-mail communications we reviewed, the NSLB attorney assigned to this case stated that it was unnecessary to establish probable cause since the [redacted]

(S)

[redacted]

The NSLB attorney noted that the [redacted] would accept an NSL for [redacted] but decided not to issue an NSL because of concerns that [redacted]

(S)

The second substantive issue was whether [redacted] was associated with a terrorist organization and therefore whether the records were relevant to a national security investigation. [redacted]

(S)

[Redacted]

(S)

According to the FBI agent [redacted]

[Redacted]

²⁹ A Section 215 order may be issued for a tangible thing that is also obtainable pursuant to a grand jury subpoena or court order directing the production of records or tangible things. 50 U.S.C. § 1861 (c)(2)(D). (U)

(S)

[Redacted]

(S)

6. Request for [redacted]

b1

An FBI agent submitted a Section 215 request for records related to

(S)

[redacted] counterterrorism case. The Section 215 request was generated at FBI Headquarters [redacted]

(S)

[redacted]

This request was processed in 72 days. After reviewing the read application and order, the FISA Court requested that OIPR revise the application and order to more precisely identify the records requested. [redacted]

(S)

[redacted]

Section 215 requires that orders describe the records requested with "sufficient particularity to permit them to be fairly identified." 50 U.S.C. § 1861(b)(2)(A). ~~(S)~~

(S)

The case agent told the OIG that he provided the [redacted] with [redacted] over 1 month before the defendants pled guilty and 4 months after the trial was originally scheduled to begin. According to the case agent, some of the delay in obtaining the business records occurred because the request [redacted]

(S)

[redacted]

(S)

Because [redacted] was not provided until after the trial began and a month or two before the defendants pled guilty, the agent told us that he did not think the records were used at the trial. The agent also told the OIG [redacted]

(S)

[redacted]

The agent told the OIG that the records produced in response to the Section 215 order were not relevant to any FBI investigations of U.S. persons. ~~(S)~~

(S)

7. Request for [redacted]

An FBI agent submitted a Section 215 request in a counterterrorism investigation [redacted]

(S)

[redacted]

(S)

31

[redacted]

(S)

[Redacted]

(S)

This Section 215 request was processed in 212 days. According to the NSLB attorney who handled the matter, the agent who submitted the request established the relevance of the [Redacted] records for [Redacted]

[Redacted] but did not provide any information to establish the relevance of the records for [Redacted]

Although the agent eventually persuaded the NSLB attorney to include [Redacted] because the subject was in telephone contact with [Redacted] OIPR raised a concern [Redacted]

[Redacted] After discussions between the NSLB attorney and an OIPR supervisor, OIPR submitted to the FISA Court an application for [Redacted] and omitted [Redacted] but included [Redacted]

This request was further delayed when it was not properly entered into the FISAMS, OIPR added and then removed detailed facts from a related FISA application, the assigned OIPR attorney went on vacation, and OIPR modified the Section 215 template to conform to the requirements of the newly enacted Reauthorization Act. (U)

(S)

In response to this Section 215 order, [Redacted]

[Redacted] The agent told the OIG that the information received from the Section 215 order did not show evidence of terrorist activities, but that obtaining the information helped close a lead.

~~(S)~~

(S)

8. Request for [Redacted]

~~(S)~~

(S)

An FBI agent submitted a Section 215 request in a counterterrorism investigation [Redacted]

(S)

[Redacted]

The Section 215 request was processed in 604 days. According to an NSLB attorney's e-mail, the draft application was sent to OIPR 1 year before the OIPR attorney began communicating with NSLB about the request. The former Acting Counsel for Intelligence Policy told the OIG that on several occasions during the first year the Section 215 application was pending at OIPR, she spoke to the FBI Deputy General Counsel regarding the status of the application. In an e-mail to NSLB from OIPR, the OIPR attorney expressed concerns that the application lacked a nexus to terrorism. OIPR requested additional information regarding the request, such as an [Redacted]

(S)

[Redacted]

(S)

In response to the Section 215 order, the agent received records [Redacted] However, the agent did not receive information [Redacted]

[Redacted]

(S)

9. and 10. Requests for [Redacted]

(S)

An FBI agent submitted [Redacted] Section 215 requests for [Redacted] [Redacted] as part of a counterterrorism investigation. The requests were deemed urgent based on the serious and credible nature of the threat reported. [Redacted]

[Redacted]

(S)

(S)

[Redacted]

(S)

[Redacted]

(S)

The Section 215 request for [Redacted] was processed in 10 days. The Section 215 request for [Redacted] was processed in 17 days.

[Redacted]

³³ The FBI then requested full FISA orders for the information, but NSLB suggested seeking Section 215 orders instead.

[Redacted]

The agent received no records in response to the Section 215 orders.

(S)

According to the agent, [Redacted] and the agent had initiated his Section 215 request approximately 6 months after the time period he was investigating.

~~(S)~~

(S)

11. Request for [Redacted]

(S)

An FBI agent submitted a Section 215 request for [Redacted] intelligence investigations.

[Redacted]

³³ 18 U.S.C. § 2709 authorizes NSLs for subscriber information and toll billing records information, or electronic communication transactions records. (U)

This request was processed in 137 days. After reviewing the read application and order, the FISA Court requested that OIPR extend the time for the provider to produce the records from 20 to 30 days. (U)

According to the case agent, upon receipt of the records [redacted]

b1

(S)

[redacted]

[redacted] Nevertheless, the case agent stated that the information was useful because it closed the lead and corroborated other information. ~~(S)~~

B. Section 215 Requests that were Withdrawn (U)

In the following section, we describe the six withdrawn Section 215 requests. We discuss the type of records requested, the processing time, and the reason the request was withdrawn. Based on our interviews and document review, we identified two primary reasons for the withdrawal of FBI requests for Section 215 applications: the request lacked sufficient predicate or the provider did not maintain the records requested.³⁴ We also identify whether the request was withdrawn at NSLB or OIPR. (U)

1. Request for [redacted]

(S)

An FBI agent submitted a Section 215 request [redacted]

(S)

[redacted] in a counterterrorism case. [redacted]

[redacted]

This Section 215 request was withdrawn from OIPR by the FBI after 434 days. [redacted]

(S)

[redacted]

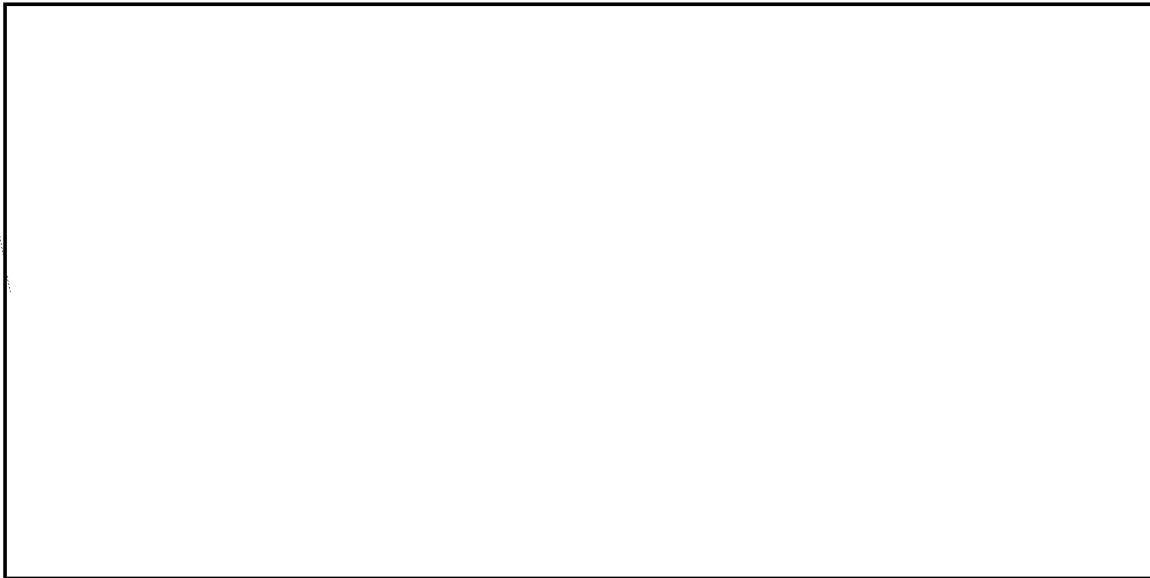
[redacted] The Section 215 request was presented to the FISA Court as a read copy application on two

³⁴ We use the term "primary reason" because two investigations changed course while NSLB or OIPR attorneys were working with FBI agents to develop sufficient information to support the request. We consider the change of course to be a secondary reason because both cases changed course before the FBI case agents provided the information required by NSLB or OIPR to submit the Section 215 request to the FISA Court. (U)

occasions. On both occasions, the FISA Court indicated it would not sign the order because of First Amendment concerns. ~~(S)~~

b1

(S)



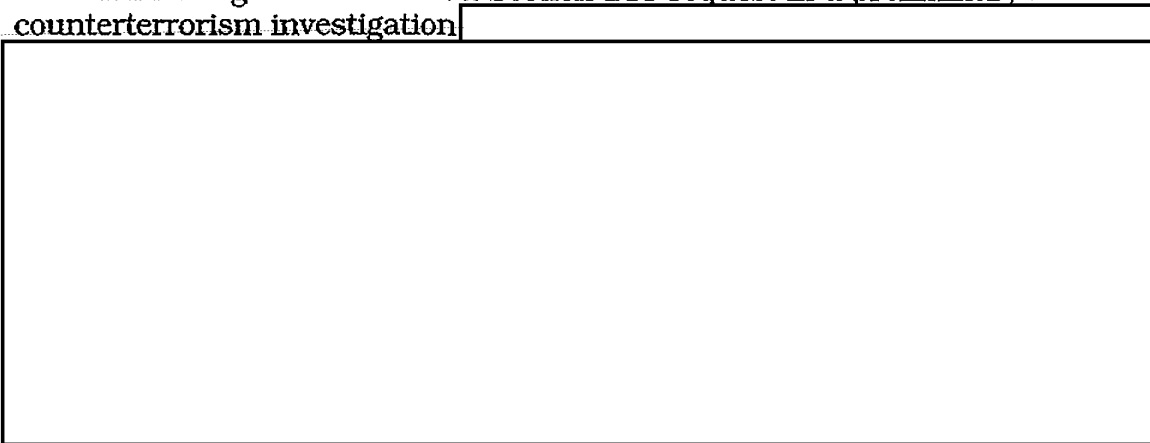
(S)

2. Request for Rental



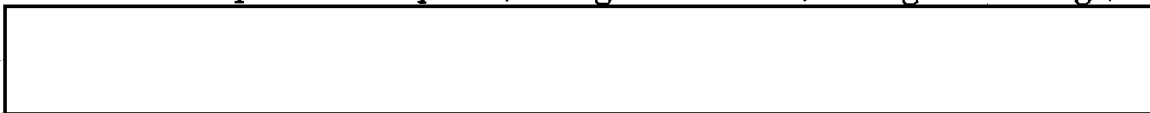
(S)

An FBI agent submitted a Section 215 request in a preliminary counterterrorism investigation



(S)

This Section 215 request was withdrawn from NSLB by the FBI after 426 days. Prior to it being withdrawn, the NSLB attorney sent several e-mails to the agent requesting additional information to support the Section 215 request. In response, the agent indicated, among other things,



FBI e-mail indicates that the General

³⁵ We discuss this case in detail in Chapter Six at pages 65-74. (U)

Counsel and Deputy General Counsel for NSLB "legally killed" the Section 215 request.³⁶ ~~(S)~~

b1

(S) 3. Request for [redacted]

(S) An FBI agent submitted a Section 215 request in a counterterrorism investigation [redacted]

FBI agent e-mailed FBI Headquarters and confirmed that he was pursuing the Section 215 business record request. ~~(S)~~

This Section 215 request was withdrawn from NSLB by the FBI after 608 days. The case agent told the OIG that FBI Headquarters informed him that the case would not be approved because the subject was a naturalized U.S. citizen and there was no connection to a foreign power. Although this request was initially provided to OIPR without prior approval by the NSLB attorney, it subsequently was re-routed to and later withdrawn at NSLB. (U)

(S) 4. Request for [redacted]

(S) An FBI agent submitted a Section 215 request in a counterterrorism investigation [redacted]

[redacted] decided to try the Section 215 request since he had not previously used this investigative tool. ~~(S)~~

This Section 215 request was withdrawn from NSLB by the FBI after 160 days. The request was withdrawn after several e-mails from the NSLB attorney to the case agents.³⁷ In the e-mails, the NSLB attorney identified several concerns regarding the request, including [redacted]

(S) [redacted]

³⁶ In addition, an e-mail from the assigned NSLB attorney indicates that the FBI Deputy General Counsel questioned whether the investigation was properly opened. (U)

³⁷ NSLB was in contact with two case agents because the case was reassigned while the application was pending. (U)

(S) [Redacted]

Eventually, the case agent to whom the investigation had been transferred asked to withdraw the request because he did not see the need for the records requested. ~~(S)~~

(S) 5. Request for [Redacted]

(S) An FBI agent submitted a Section 215 request in a cyber-terrorism investigation [Redacted]

[Redacted]

This Section 215 request was withdrawn from NSLB by the FBI after 186 days when the agent learned that the provider did not maintain the records requested. (U)

(S) 6. Request for [Redacted]

(S) An FBI agent submitted a Section 215 request for [Redacted] as part of a counterintelligence investigation. The

[Redacted]

(S) This Section 215 request was withdrawn from OIPR by the FBI after 58 days when the agent learned that the [Redacted]

II. Combination Section 215 Requests (U)

(S) As previously discussed, as a result of the March 2006 Reauthorization Act, combination orders for subscriber information became unnecessary and OIPR ceased preparing combination orders for [Redacted]. Therefore, in 2006 combination orders were submitted to the FISA Court only from January 1 through March 8, 2006. Below we present a brief overview of the use of combination orders. We also describe the modifications or handwritten notations by the FISA Court to those orders.

~~(S)~~

A. Use of Combination Orders (U)

(S) [Redacted]

ACLU Sect. 215-1508

(S)

[Redacted]

Combination applications are drafted at OIPR and after they are signed by the FISA Court, the orders are sent to the field office nearest the custodian of records for service. The most common combination order is for subscriber information, which identifies the person whose phone was used to contact the subject of an investigation. The subscriber information is only for records that are maintained by the communication provider upon whom the order was served. If the phone number of interest belongs to another provider, other investigative tools such as NSLs can be used to obtain the subscriber information related to that phone number.

(S)

[Redacted]

(S)

Combination orders are also used to obtain [Redacted] Four agents told us that they received [Redacted] as directed by the FISA Court in 2006. Of the four agents who said they received [Redacted] [Redacted] only two told us that the information was helpful. One agent told us that the [Redacted]

[Redacted]

(S)

Two agents told us the [Redacted] was not useful. [Redacted]

[Redacted]

The other agent said he never attempted to utilize the information because his subject moved out of the country. ~~(S)~~

As we noted in our March 2007 report, agents were not always aware when OIPR added a business record request to their pen register/trap and trace request. We spoke to agents who submitted both initial and renewal requests for pen register/trap and trace orders in 2006. Many agents who submitted initial requests could not tell us whether OIPR added a business record to their pen register/trap and trace requests or whether they received subscriber information pursuant to the order. Agents who submitted

³⁸ Telephone Applications is an investigative tool that also serves as the central repository for all telephone data collected during the course of FBI investigations. (U)

renewal applications were more likely to be aware of the addition of the business record. If an agent is not aware of the addition of the business record request and the provider does not produce the information required in the court order, then the agent does not know to enforce the Section 215 order. (U)

B. Modifications and Notations to Combination Orders (U)

The following section describes the number of Section 215 applications and orders modified by the FISA Court. We identified modifications or notations on four combination orders. (U)

The FISA Court handwrote modifications or notations on four combination applications and orders in 2006. With regard to one combination order, the FBI had informed the FISA Court that it received records in response to, but beyond the scope of, the FISA Court order but had not provided the additional material to OIPR when the FBI sought to renew the order. The FISA Court modified the order to require that the FBI provide the material to OIPR by a specific date. (U)

The second combination order contained a handwritten correction to the expiration date of the Court's order. Although the application correctly stated the order would expire in 90 days, the month of the expiration date in the order was incorrect and the FISA Court modified the order so that the month correctly reflected the 90-day duration of the order. (U)

The remaining two combination orders requested [redacted]

(S)

b1

[redacted] The Court's handwritten notations on the two combination orders reference the Court's opinion. ~~(S)~~

CHAPTER FIVE OIG ANALYSIS (U)

In this chapter, we provide our analysis of FBI requests for Section 215 orders processed in 2006. In addition, as required by the Reauthorization Act, we discuss bureaucratic and other impediments to obtaining a Section 215 order, FISA Court modifications to the applications and orders, and the use and effectiveness of the information received pursuant to the Section 215 orders. (U)

I. Delays in Implementing Section 215 Authority and Other Impediments to Use (U)

The Reauthorization Act directed the OIG to identify bureaucratic or procedural impediments that negatively affected the FBI's ability to obtain Section 215 orders. In this section, we identify the processing time for Section 215 requests in 2006 and then compare our findings for 2006 to the findings in our previous report, which covered Section 215 requests from 2004 through 2005.³⁹ We then discuss the causes for the delays. (U)

A. Pure Section 215 Processing Times in 2006 (U)

In order to calculate the processing time for each Section 215 request in 2006, we sought to determine how long each request was pending at an FBI field office, FBI Headquarters, and OIPR. Initially, we expected to identify the relevant dates through the FBI's FISA Management System (FISAMS) and OIPR's OASIS case management database, the FISA tracking systems used by the FBI and OIPR. However, we learned that the dates recorded in the FBI and OIPR tracking systems were not always reliable. For example, Section 215 requests were not always entered into FISAMS when they were actually initiated in the FBI field office. Other requests were initiated at FBI Headquarters and entered into FISAMS at an arbitrary future date. When this occurred, FISAMS reflected the date the request was entered into the system as opposed to the actual initiation date. For example, FISAMS indicates that one particular Section 215 request was first initiated more than 2 weeks after the FISA Court signed the order. FISAMS also indicates that another Section 215 request was initiated after NSLB sent a completed draft application to OIPR. (U)

Similarly, OIPR's tracking system does not always contain accurate processing dates. For example, OASIS reflects the date on which OIPR first receives an application from FBI Headquarters. However, FBI Headquarters erroneously sent three requests to OIPR before the Section 215 applications

³⁹ The first Section 215 request was approved in 2004. (U)

and orders were drafted and approved by NSLB. As a result, these three requests were returned to NSLB for drafting and approvals. OASIS shows the date that OIPR received the misdirected request and not the date it received and began reviewing the draft Section 215 application and order approved by NSLB.⁴⁰ (U)

Therefore, the dates we relied upon to identify the processing time for Section 215 applications in 2006 reflect information from our interviews of FBI and OIPR staff, contemporaneous e-mails, and the FBI and OIPR tracking systems. (U)

As used in this report, the "processing time" for a request includes the number of days that elapsed from the date the agent initiated the Section 215 business record request to the date the request was signed by the FISA Court or withdrawn. We did not include the time required to serve the order on the recipient in our processing time calculation because that information was not available for each request. (U)

Chart 5.1 illustrates the total processing time for the 11 of the 15 approved Section 215 orders processed in 2006. The chart provides the processing time for each entity involved in the process. The chart does not include [redacted]

(S)

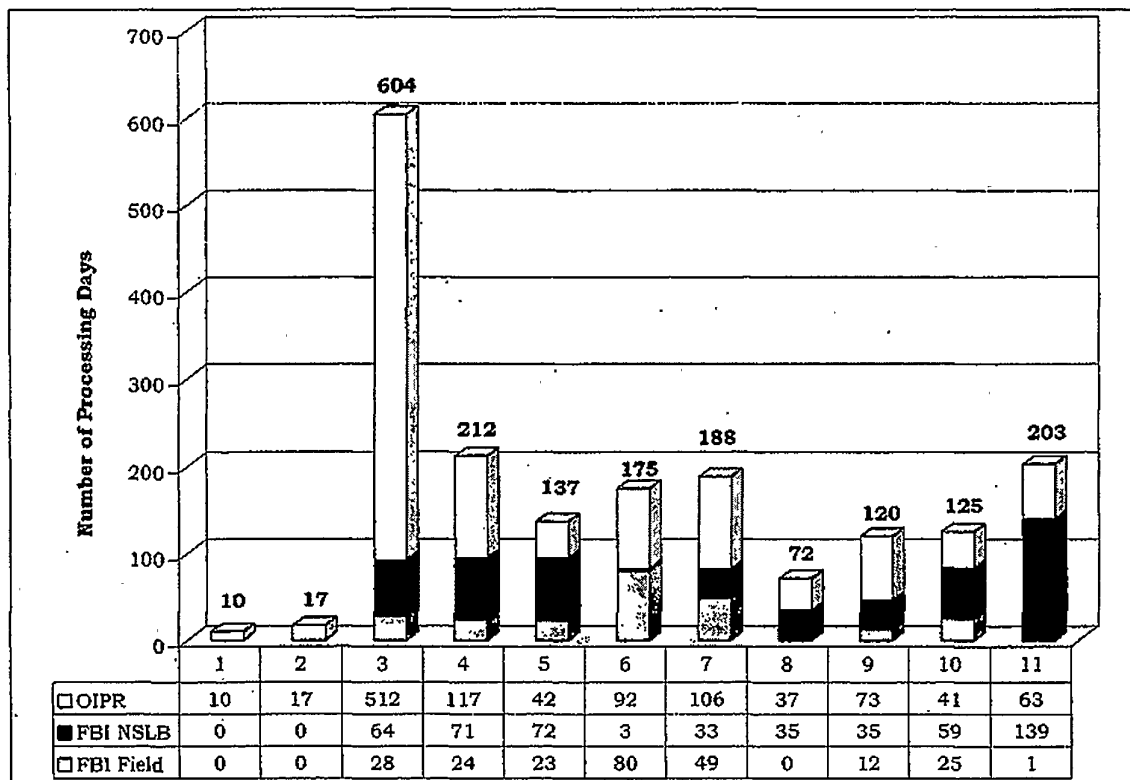
b1

⁴⁰ In addition, in 2006 neither the FBI's nor OIPR's tracking systems included information that tracks applications related to [redacted] OIPR began to include a reference to applications related to [redacted] in 2007 after the OIG questioned how OIPR could accurately track and report the total number of Section 215 applications in its semi-annual reports to Congress if the recordkeeping system did not include applications related to [redacted]

(S)

(S)

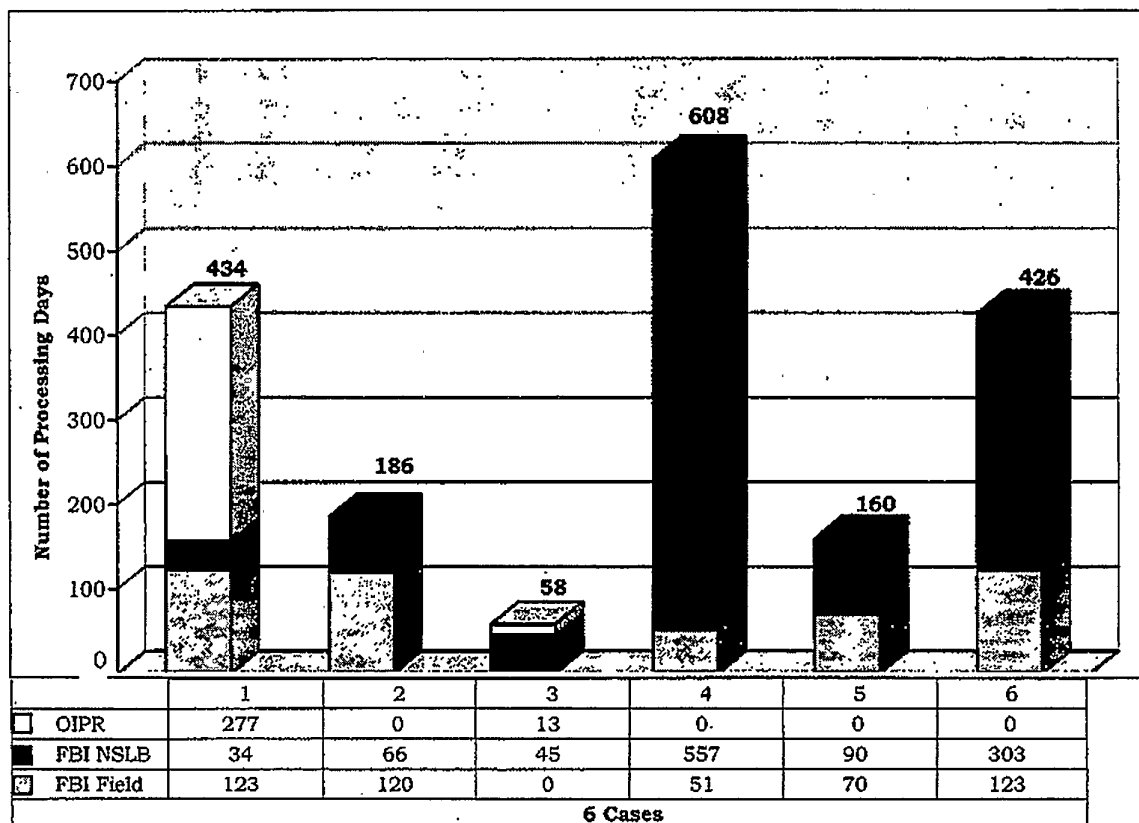
CHART 5.1
Processing Time for 11 "Pure"
Section 215 Requests Processed in 2006 (U)



Source: FBI and OIPR (U)

Chart 5.2 illustrates the total processing time for the six withdrawn requests processed in 2006. (U)

CHART 5.2
Processing Time for Six Withdrawn "Pure" Section 215 Requests Processed in 2006 (U)



Source: FBI and OIPR (U)

NSLB and OIPR attorneys told us that the experience both agencies have gained in handling Section 215 requests resulted in efficiencies in the review and approval process. By 2005, NSLB and OIPR had assigned specific attorneys to process the business record applications in their respective offices. The dedicated FBI and OIPR attorneys developed a procedure and a working relationship that allowed them to process business record applications more efficiently.⁴¹ (U)

⁴¹ The process has since changed at both the FBI and OIPR. In early 2007, the FBI decided not to dedicate a specific attorney to Section 215 requests and now assigns routine requests to one of four designated attorneys who either provide a preliminary draft of the business record application to OIPR or assist a colleague in doing so. In addition, in October 2007 the OIPR attorney assigned to Section 215 requests left OIPR and OIPR assigned the Section 215 responsibilities to two other attorneys. (U)

ACLU Sect. 215-1514

However, we found that several requests were delayed at FBI Headquarters in 2006 because they were prematurely sent to OIPR, held up by the substantive unit at FBI Headquarters, or assigned to the wrong NSLB attorney. We also found some processing delays at OIPR as well. We discuss both types of processing delays in the following section. (U)

B. Pure Section 215 Processing Times 2004-2006 (U)

The FBI and OIPR processed 21 pure Section 215 requests in 2006.

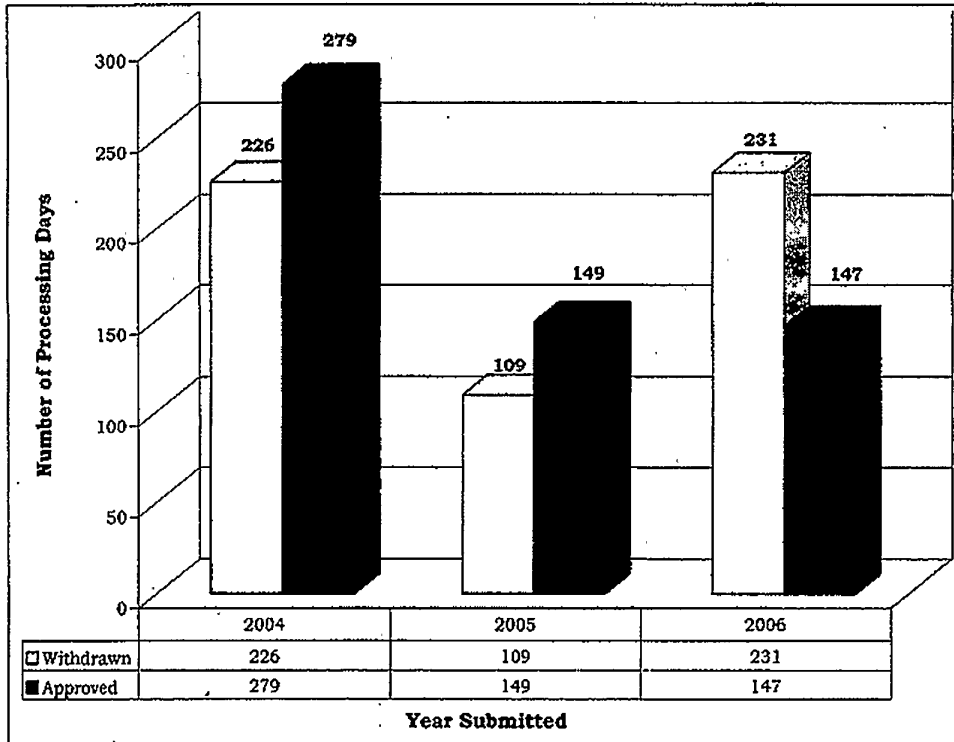
(S) In this section, we discuss only 17 of the 21 applications.

b1

The processing time for these requests ranged from 10 days to 608 days, with an average of 169 days for the approved orders and 312 days for the withdrawn requests. These statistics are not directly comparable to those in our previous report because we have included the time spent preparing the application in an FBI field office in our calculations for 2006. ~~(S)~~

However, if we exclude FBI field office time, the 2006 processing time average is 147 days for approved orders and 231 days for withdrawn requests. Chart 5.3 illustrates the combined FBI Headquarters and OIPR processing time for Section 215 requests from 2004 through 2006, excluding FBI field time. Chart 5.3 shows that the processing time for approved Section 215 requests has decreased each year since 2004, although the processing time for withdrawn requests rose in 2006. (U)

CHART 5.3
FBI Headquarters and OIPR Average Processing Time
for Section 215 Requests from 2004 through 2006* (U)



Source: FBI and OIPR (U)

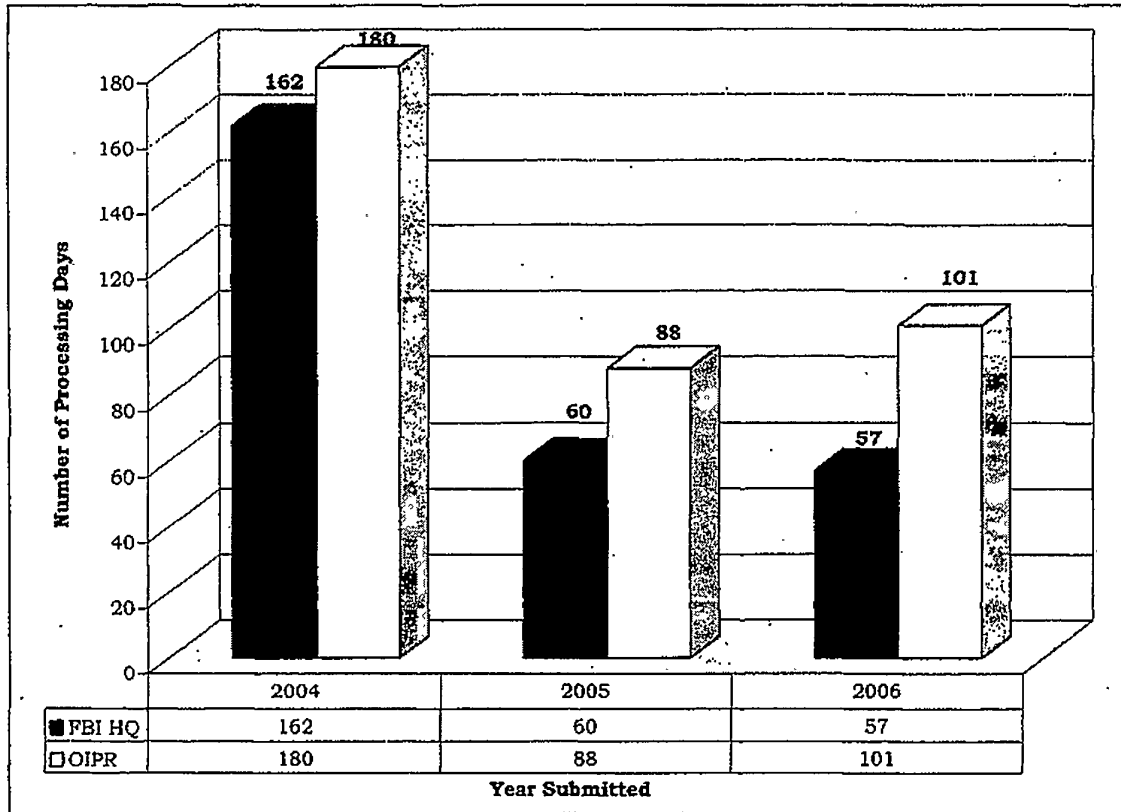
(S) *Note: Chart 5.3 includes the four Section 215 orders processed in 2006 and signed in 2007 and excludes [redacted]

b1

Eleven Section 215 orders were processed in 2006 and approved by the FISA Court. The average processing time at FBI Headquarters and OIPR for applications that resulted in orders from 2004 through 2006 is illustrated in Chart 5.4. Chart 5.4 illustrates that FBI Headquarters and OIPR processing time decreased significantly from 2004 to 2005 and has remained relatively constant in 2005 and 2006. Processing time in OIPR increased slightly in 2006.⁴² (U)

⁴² We did not compare the average processing time for withdrawn requests between the FBI and OIPR because the FBI determines when and if to withdraw a request. (U)

CHART 5.4
FBI Headquarters and OIPR Average Processing Time for Section 215
Orders from 2004 through 2006* (U)



Source: FBI and OIPR (U)

*Note: Chart 5.4 includes the four Section 215 orders processed in 2006 and signed in 2007 and excludes

(S)

b1

We identified the same reasons for processing delays in 2006 as we described in our previous report – some FBI employees’ unfamiliarity with Section 215, too few resources, the multi-layered review process, and substantive issues regarding statutory interpretation. (U)

We discuss both the procedural and substantive delays below. (U)

C. Bureaucratic and Procedural Impediments (U)

1. FBI Employees’ Unfamiliarity with Section 215 Requests and the Approval Process (U)

Our review determined that FBI employees’ unfamiliarity with Section 215 requests was the primary cause of the delays that occur from the time a case agent initiated a Section 215 request until the time the request was assigned to the NSLB attorney responsible for business record applications. (U)

ACLU Sect. 215-1517

~~SECRET~~

As previously noted, in order to initiate a request an agent must complete a Section 215 request form found on FISAMS which automatically directs the request through the proper chain of approvals in the field office and then to the substantive desk at FBI Headquarters. At FBI Headquarters, an NSLB supervisor assigns the request to the NSLB attorney responsible for business records. The NSLB attorney then drafts the Section 215 application package, which is reviewed by an NSLB supervisor before it is provided to OIPR. An OIPR line attorney and supervisor review and edit the Section 215 package before the "final" version is sent to NSLB for final review and signature. (U)

Most of the FBI agents we interviewed said their Section 215 request was the first submitted from their respective field office. Agents told us that because their supervisors were less familiar with Section 215 requests than with other more commonly used investigative tools such as national security letters, they took more time to review and approve each request. According to the data we collected in this review, the average processing time for Section 215 requests in FBI field offices in 2006 was 30 days. (U)

(S) We also determined that [] of the 17 Section 215 requests processed in 2006 were delayed because they were not properly routed after they were approved by the field office and sent to FBI Headquarters. Several requests were delayed because FBI Headquarters did not assign the Section 215 request to the designated NSLB attorney. For example, [] requests were delayed between 2 and 6 weeks because FBI Headquarters sent the request directly to OIPR instead of routing the request through the designated NSLB attorney.⁴³ (S)

b1

Another Section 215 request was delayed or misdirected at four different points before it was withdrawn. The substantive desk at FBI Headquarters did not assign the request to NSLB for approximately 2 months. NSLB assigned the request to the wrong attorney, and therefore the request was delayed for an additional 11 months. The same request was then sent to OIPR before NSLB reviewed, drafted, and approved the application. One month after the request was returned to OIPR, the request was assigned to the appropriate NSLB attorney, who was then told by the substantive desk not to work on the package until further notice. The substantive desk withdrew the request for the Section 215 order approximately 10 weeks later. (U)

⁴³ As of July 2007, the FBI FISAMS included an automated work flow for business records requests. The FBI stated that the dedicated work flow should reduce the routing errors discussed above. (U)

ACLU Sect. 215-1518

46
~~SECRET~~

2. OIPR Resources (U)

According to e-mail traffic we reviewed, several delays in submitting Section 215 applications by OIPR were attributable to the fact that during 2006 business record applications were assigned to a single OIPR attorney who had other responsibilities. As of November 2007, OIPR had two attorneys assigned to process business records but both attorneys have other responsibilities. (U)

3. Multi-Layered Review Process (U)

Since our last report, the multi-layered review process for 215 applications has not changed. As a result, Section 215 requests may be delayed at any one of several levels. We found delays at the field office level, at FBI Headquarters, and at OIPR. (U)

For the most part, the multi-layered review process is self-imposed because the only statutorily required review is that of the FISA Court. The other multiple levels of review leading to submission of an application to the FISA Court were established by DOJ and the FBI. OIPR reviews all Section 215 applications because OIPR attorneys present the applications to the FISA Court. According to OIPR, the FISA Court Rules of Procedures provide that the Attorney General determines who is permitted to appear before the FISA Court, and FBI attorneys have not been authorized by the Attorney General to practice before the FISA Court for this purpose. In turn, the FBI requires that its NSLB attorneys draft the applications because Section 215 provides that only the FBI Director or his designee may apply for a Section 215 order.⁴⁴ (U)

At the field level, the multiple levels of approval are similar to those required for other investigative tools, including NSLs and other FISA Court applications. (U)

We found that inefficiencies caused by the FBI's and OIPR's multi-layered review process are magnified by the general nature of the Section 215 request. Because the standard for a business record request is relevance, Section 215 applications do not contain the detailed factual allegations found in other FISA applications that require a showing of probable cause, a higher evidentiary standard. In order to better understand the request, reviewers at the FBI, OIPR, and the FISA Court

⁴⁴ The Director of the FBI has delegated to the following FBI officials the authority to apply for a Section 215 order: the FBI General Counsel; the FBI Deputy Director; the Executive Assistant Director for National Security; the Assistant Directors and Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; the Deputy General Counsel for National Security Affairs; and the Senior Counsel for National Security Affairs. (U)

often have questions about details of the investigation that are not always included in the initial application. Many of the questions may have already been asked by other reviewers, but the answers are not incorporated into the application because of the low standard of review. As a result, the review process can be slower when different reviewers ask similar questions about the application. (U)

D. Substantive Delays (U)

In addition to delays inherent in a multi-layered review process, many of the delays are also attributable to the issues presented by individual Section 215 requests. Of the 17 approved and withdrawn Section 215 requests processed in 2006 and described in the body of this report, [redacted] were delayed because they raised substantive issues regarding the nature of the records and [redacted] raised concerns regarding whether the application met the statutory requirements. ~~(S)~~

b1

1. Nature of the Record (U)

(S) [redacted] of the requests were delayed because they involved unique substantive issues. [redacted]

(S) [redacted] request raised a question as to whether a federal inmate's [redacted] were business records within the meaning of Section 215. [redacted] also raised a concern about the relevance of the request to international terrorism because the FBI did not know if [redacted] a request for records from an [redacted] raised an issue regarding whether it was appropriate to use a Section 215 request to determine if a company was an entity on which an NSL could be served. [redacted] Section 215 request for [redacted] raised concerns because of its scope and [redacted]

(S) Each of these [redacted] requests raised new issues that took significant time to research, negotiate, and resolve. On average, the total processing time for these [redacted] requests was 162 days. ~~(S)~~

2. The Statutory Requirements (U)

(S) In addition, we found that FBI Headquarters or OIPR attorneys raised concerns that [redacted] of the 17 applications did not meet the statutory requirements. When NSLB or OIPR attorneys have questions about a

request, they may contact each other, their supervisors, or the case agent. The resulting dialogue can affect the timing of the request. ~~(S)~~

b1

(S) In [redacted] instances, the requests were eventually withdrawn for lack of predicate, with [redacted] withdrawn at NSLB, [redacted] withdrawn at OIPR after [redacted].
[redacted]
[redacted] ⁴⁵ The FISA Court granted Section 215 orders for the [redacted] applications. ~~(S)~~

a. Requests Withdrawn at NSLB (U)

(S) As noted above, [redacted] of these requests were withdrawn at NSLB. Before the requests were withdrawn, the FBI discussed the case with the case agent, and either the agent decided to withdraw the request on his own initiative or FBI Headquarters told the agent the request would not be approved. One case involved a request for information [redacted] and the case agent agreed to withdraw the request on his own initiative. With regard to the requests [redacted] the agents did not agree to withdraw the requests until after FBI Headquarters told them that their applications would not be approved. The average processing time for these [redacted] requests was 398 days. ~~(S)~~

b. Requests Withdrawn at OIPR (U)

The single request withdrawn at OIPR was withdrawn by the FBI after the FISA Court declined to approve the application on two occasions. The former Acting Counsel for Intelligence Policy told the OIG that pursuant to the FISA statute, only the FBI is permitted to withdraw a FISA request. The former Acting Counsel cited Section 104(e)(1) of the FISA statute, which provides that the Director of the FBI may request that a FISA application be reviewed by the Attorney General if the Director states in writing that the FISA application meets the requirements in the statute. The former Acting Counsel stated that as a practical matter this provision requires that OIPR either work with the FBI until OIPR determines that the FISA request meets the statutory requirements or the FBI consents to withdraw the request.⁴⁶
(U)

⁴⁵ Only two other Section 215 requests were withdrawn. Both were withdrawn after the agent learned that the provider did not maintain the records requested. A request for information [redacted] was withdrawn at NSLB, while a request for [redacted] was withdrawn at OIPR. ~~(S)~~

(S)

[redacted]

This policy may account in part for the processing time of requests for which OIPR identified concerns about whether they met statutory requirements. Of the 17 pure Section 215 requests processed in 2006, OIPR raised statutory concerns regarding [redacted]

b1

(S)

[redacted]

[redacted] On average, these requests were processed in 416 days. ~~(S)~~

E. Expedited Requests (U)

Two of the requests processed in 2006 were expedited by the FBI and OIPR. These two requests show that when the FBI identifies the need to expedite a Section 215 request, both the FBI and OIPR can expedite the task. The two requests, [redacted] were expedited because of a serious security threat and were processed in 10 and 17 days, respectively. ~~(S)~~

(S)

F. Unremarkable Applications (U)

[redacted] requests did not seek sensitive records, raise statutory questions, or involve exigent circumstances [redacted] were signed by the FISA Court. [redacted] was a request for [redacted] [redacted] withdrawn once the agents learned the providers did not maintain [redacted] On average, these requests were processed in 113 days. ~~(S)~~

(S)

II. Modified Pure and Combination Section 215 Orders (U)

As required by the Reauthorization Act, we also reviewed how many times the FISA Court modified Section 215 orders. We examined information about the number and types of modifications for both pure and combination Section 215 orders discussed in the body of this report. We reviewed each Section 215 pure and combination order for handwritten changes signed by the FISA Court judge. In addition, we reviewed OIPR documents and e-mails and asked OIPR officials about revisions to Section 215 applications made at the request of the FISA Court. (U)

We found that the FISA Court modified four combination and five pure Section 215 applications and orders. We determined that six of the nine modifications were for substantive reasons. (U)

ACLU Sect. 215-1522

As noted in our first Section 215 report, OIPR considers modifications to be limited to the handwritten changes to orders made by FISA Court judges at the hearings in which the orders are signed. OIPR does not consider revisions to applications and orders made at the request of the FISA Court after it reviewed read copies to be modifications. In this review, we consider each handwritten notation or required revision to a Section 215 submission to be a modification. (U)

A. Handwritten Modifications (U)

The FISA Court made handwritten modifications to no pure Section 215 orders in 2006. It modified four combination orders. Two of the handwritten modifications to combination orders were substantive. One required the FBI to provide OIPR with information to be sequestered with the FISA Court by a specified date. OIPR had previously notified the Court that it received records in response to, but beyond the scope of, one of the Court's previous orders in the same matter, but had not sequestered the information with the Court prior to requesting that the application be renewed. The second handwritten modification corrected the expiration date of the Court's order to reflect the 90-day duration requested in the application. Although the application correctly stated the order would expire in 90 days, the month of the expiration date in the order was incorrect and the Court modified the order so that the month correctly reflected the 90-day duration of the order. (U)

(S) The other two handwritten modifications were made to combination orders [redacted]. These orders were signed the same day the Court issued an opinion holding that [redacted]. The Court's handwritten notations referenced the Court's opinion. (S)

b1

B. Revised Applications and Orders (U)

After reviewing the read copies of the 11 approved pure Section 215 orders discussed in the body of this report, the FISA Court required revisions to 5 of the applications.⁴⁷ Four of the five were substantive revisions. (U)

(S) One revised application and order related to the request for [redacted]

(S) ⁴⁷ We do not include [redacted]

ACLU Sect. 215-1523

(S)

[Redacted]

(S)

In another case, the Court required that an application be revised to describe the requested records more precisely. The request was for [Redacted]

[Redacted]

[Redacted] Section 215 requires that orders describe the records requested with "sufficient particularity to permit them to be fairly identified." See 50 U.S.C. § 1861(b)(2)(A). ~~(S)~~

A third application and order was revised to extend the time for the provider to produce the records from 20 to 30 days. (U)

(S)

A fourth application was revised to include [Redacted]

[Redacted]

Revision to a fifth application was a stylistic change that we did not find to be substantive. (U)

III. Use and Effectiveness of Information Obtained from Section 215 Orders (U)

The Reauthorization Act also directed that the OIG analyze the use and effectiveness of Section 215 as an investigative tool. In this section, we describe how the information produced pursuant to pure Section 215 orders was used in the investigation for which it was requested and whether the information was disseminated to the intelligence community or used in any criminal proceeding. (U)

A. Use in Investigations (U)

(S)

The FBI received records in response to [Redacted] of the 11 pure Section 215 orders processed in 2006, approved by the FISA Court, and discussed in the body of this report.⁴⁸ FBI agents told the OIG that the records were used to [Redacted]

[Redacted] support future FBI investigative requests, and investigate leads. Most of the agents we interviewed said the records obtained fell in the last category and that the records typically provided negative information, meaning they did not provide additional investigative information but helped close a lead. Agents also stated that investigatory efforts that result in negative information are important and not unusual. ~~(S)~~

(S)

⁴⁸ We do not include [Redacted]

(S)

(S) 1. [redacted]

(S) [redacted] Section 215 requests were initiated by the FBI after [redacted]
[redacted]
[redacted] These applications requested records of
[redacted]

2. Support Additional Investigative Requests (U)

(S) [redacted] Section 215 requests were initiated to gather information to support future requests for information. [redacted]
[redacted]
[redacted] The agent received [redacted] but told us that because of the additional records and the size [redacted] he has not yet been able to review the records produced. [redacted] Section 215 request for [redacted]
[redacted]
[redacted] The agent working on the matter said the records were useful because they contained information that enabled him to limit [redacted] [redacted] which saved him time and decreased the risk of compromising the investigation. (S)

3. Investigate Leads (U)

(S) [redacted] Section 215 requests were submitted in order to investigate leads. Of the [redacted] requests, agents received records in response to [redacted] In the remaining [redacted] requests, the providers did not maintain records for [redacted]

a. Requests for which Records Were Received (U)

(S) FBI agents said that records from the [redacted] Section 215 requests were used to investigate leads. Three agents said the records obtained were helpful and two said they were not. The agents who requested [redacted] [redacted] told us that the records were not helpful. These agents said that while they used the records to follow and close leads, the information was not what they had hoped to

(S) receive. As discussed above, the agent who requested [redacted]

(S) In contrast, FBI agents who requested records [redacted] told the OIG that the records were helpful in closing leads. [redacted]

b. Requests for which No Records Were Received (U)

(S) [redacted] Section 215 requests for which no records were received were [redacted] requests for [redacted] According to the agent, [redacted] and the Section 215 request was initiated over 6 months after the time period for which the information was requested. ~~(S)~~

B. Dissemination (U)

(S) We found that the FBI disseminated information obtained from pure Section 215 orders [redacted]

C. Use in Criminal Proceedings (U)

We did not identify any use in a criminal proceeding of records obtained from the Section 215 requests processed in 2006.⁴⁹ (U)

⁴⁹ As noted in our previous report, the FISA statute requires that the Attorney General approve the use of FISA information in criminal proceedings if the information is obtained from electronic surveillance, physical searches, or pen register/trap and traces. The FISA statute does not require that the Attorney General grant use approval for business records. (U)

OIPR attorneys raised several concerns regarding the lack of use authority for business records, including the fact that use authority may ensure that coordination among members of the intelligence community occurs and sensitive sources are not compromised. In contrast, the FBI General Counsel said she was not concerned with the lack of use authority for business records because these records have an independent existence and may be obtained in many different ways. (U)

IV. Effectiveness of Section 215 (U)

b1

(S)

[Redacted]

[Redacted] Our analysis in this section does not address the use of Section 215 [Redacted]

With regard to Section 215 uses described in the body of this report, we found that Section 215 can be a valuable investigative tool, but often is impractical because of the time it takes to obtain such an order. (U)

A. Use of Section 215 Orders (U)

Section 215 can be an impractical tool because of the lengthy time involved in developing, reviewing, and presenting the requests to the FISA Court. While no FBI agent we interviewed identified any harm to national security because of delays in the Section 215 process, many agents linked the value of Section 215 orders as an investigative tool to its efficiency as well as its effectiveness. As discussed below, several agents told us that they have other investigative tools available to them which in some cases can produce the same or comparable information more quickly. (U)

1. Other Investigative Options (U)

FBI agents told us that if delays in obtaining Section 215 orders caused their investigations to stall, they would seek the information through other means. Agents told us that they have other investigative tools available to them to obtain certain business records more quickly and with much less effort. Furthermore, one Special Agent in Charge of an FBI field office stated that in many instances agents are seeking information rather than a specific document; therefore, although the information may be included in a particular business record, the agent would likely seek comparable information using other faster investigative techniques. (U)

For speed, agents said they generally attempt to obtain information through voluntary compliance or an NSL. Both business record requests and NSLs can be issued in national security investigations for transactional records based on a relevance standard. Unlike business records, NSLs can be authorized by the Special Agent in Charge in a field office and do not require FBI Headquarters, OIPR, or FISA Court approval. Therefore, an NSL can be issued and the transactional records returned in a matter of weeks.

(S)

[Redacted]

(S)

[REDACTED]

NSLs however are not available for all business records. NSLs may be issued to entities such as telephone companies, financial institutions, and credit agencies to produce limited categories of customer and consumer transaction information. Section 215, in contrast, is not limited to specific categories of transactional records and can be used to obtain items which are not available through NSLs such as [REDACTED]

(S)

[REDACTED]

Another investigative tool that can be quicker than a business record request is a grand jury subpoena. Agents conducting national security investigations with a criminal nexus do not have to seek FBI Headquarters or NSLB approval to obtain a grand jury subpoena because they are issued under the signature of the prosecutor supervising the grand jury investigation. However, grand jury subpoenas also have limitations in certain contexts. The primary limitation is that the investigation must have a criminal nexus. In addition, information presented to a grand jury may be made public in subsequent court proceedings and with limited exceptions grand jury subpoenas do not obligate the recipient to maintain the secrecy of the investigation. For example, [REDACTED]

(S)

[REDACTED]

[REDACTED] told the OIG that they chose not to use grand jury subpoenas in order to maintain the secrecy of the investigations. ~~(S)~~

2. Effect of the Processing Delays (U)

According to FBI agents and supervisors we interviewed, when working on a national security investigation an agent identifies the information required and then determines the fastest legal way to obtain that information. Some agents stated that a few months may be an acceptable delay for business records because they can continue working on other aspects of their investigation during that time frame. However, agents stated that an investigation is likely to stall with a delay of 6 months to a year in obtaining records, and that if this occurred they would look for other means to obtain the information. One agent noted that a 6-month delay is a particular concern with a preliminary investigation because although extensions may be granted, a preliminary investigation is expected either to become a full investigation or be closed in a 6-month period. (U)

(S)

One agent told us that while he was waiting for a Section 215 request for [REDACTED] he obtained the equivalent information through public sources such as Google. The agent also told us that if he had received the information through the Section 215 order, he could have used the time he invested in researching public databases to work on other leads and investigations. ~~(S)~~

ACLU Sect. 215-1528

Another agent said she was too frustrated by her experience pursuing a previous Section 215 order to submit another. Instead, the agent decided to invest her time [redacted]

b1

(S) [redacted]

[redacted] The agent told us that she thinks it likely that she obtained the same information that she would have with a business record request although she said she could not be certain. The agent stated that the [redacted] was time consuming, but that she would not use a Section 215 request unless she needed something specific that she could not obtain through other means. ~~(S)~~

(S) In contrast, the agent who received [redacted] [redacted] told us that seeking the Section 215 order saved time.

The agent stated that [redacted]
[redacted]

B. Value of Section 215 Orders (U)

According to FBI agents we interviewed, when they need a particular business record and it is not available by another investigative tool, Section 215 can be an invaluable tool. [redacted] told us they could not have obtained the records for their investigations without the provision. In each case, the agents were told [redacted]

(S)

[redacted] Although no agent suggested that the records obtained pursuant to the order resulted in a major case development, many stated that every investigative tool in an FBI agent's tool box is important and that when it is the only tool that will produce the information, it is invaluable even if the process is burdensome. ~~(S)~~

V. Summary (U)

We determined that the processing time for Section 215 requests in 2006 was similar to that in 2005, with an average of 169 days in 2006 for the approved orders and 312 days for the withdrawn requests. Similar reasons to those we identified in our previous report explained the procedural delays in 2006, including the FBI's unfamiliarity with the Section 215 process, too few resources to handle requests expeditiously, a multi-layered review process, and various substantive issues regarding whether certain applications met the statutory requirements. We also found that FBI agents generally attempted to obtain records through other, quicker investigative processes, including voluntary compliance, NSLs, and grand jury subpoenas. When providers require a court order, however, agents must obtain orders through the Section 215 review process. We also

found that when the FBI identified emergency circumstances, the FBI and OIPR were able to process a Section 215 request quickly. (U)

(S) In 2006, pure Section 215 orders processed were used primarily to exhaust investigative leads. However, the FBI used Section 215 orders to obtain information [redacted] and to support other investigative requests. ~~(S)~~

b1

(S) We did not identify any instance in which information obtained from a Section 215 order was used in a criminal proceeding in 2006. In addition, [redacted] in 2006. ~~(S)~~

(S) In sum, we found, like in our previous report, that Section 215 orders can be a valuable investigative tool to obtain records that are not available through other means. However, Section 215 orders are not used frequently because of the time it takes to obtain the order. [redacted]

**CHAPTER SIX
IMPROPER OR ILLEGAL USE OF SECTION 215 AUTHORITY
AND OTHER NOTEWORTHY FACTS (U)**

The Reauthorization Act also directed the OIG to identify "any noteworthy facts or circumstances relating to orders under such section, including any illegal or improper use of the authority." In this review, we did not identify any illegal use of Section 215 authority. However, we identified two instances where the provider produced records that were in response to, but were outside the scope of, a FISA Court order. These two cases raise concerns about the FBI's identification and handling of such additional material. (U)

Also discussed in this chapter are two additional "noteworthy facts" regarding the FBI's use of Section 215 authority in 2006. The first relates to the FBI's use of a national security letter to obtain information about a subject after the FISA Court rejected a Section 215 order for records concerning the same subject based on First Amendment concerns.

(S)

b1

I. Two Instances in which the FBI Received More Information than it had Requested in Response to a Section 215 Order (U)

Through our review of FBI and OIPR documents, we identified two instances in which the FBI received more information than it had requested in response to a Section 215 order. One instance occurred in connection with a combination order and the other occurred pursuant to a pure Section 215 order. The FBI determined that the matter that involved the combination order was reportable to the President's Intelligence Oversight Board (IOB). The FBI determined that the matter that involved the pure Section 215 order was not reportable to the IOB. (U)

As discussed in detail in our March 2007 Section 215 report, the FBI is required to report any improper use of Section 215 authority to the IOB. In 1976 the IOB was created by Executive Order and charged with reviewing activities of the U.S. intelligence community and informing the President of any activities that the IOB believes "may be unlawful or contrary to executive order or Presidential Directives." See Executive Order 12863.⁵⁰ The Executive Order also requires the FBI's General Counsel to report to the

⁵⁰ For more information about the IOB, see the OIG's report titled *Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act*, pages 20-24 (March 2006). (U)

IOB on at least a quarterly basis intelligence activities the General Counsel has "reason to believe may be unlawful or contrary to executive order or Presidential directive," which are referred to as "IOB violations." (U)

A. Case 1 (U)

(S) As previously noted, combination orders are business record requests attached to pen register/trap and trace requests. We found that in one matter involving a combination order, the [redacted] that was not requested in the Section 215 application or authorized by the FISA Court order. [redacted] had been authorized and received pursuant to a previous combination order for the subject. Neither the FBI agent who had requested the pen register/trap and trace order nor OIPR, however, was aware that the [redacted] had been provided pursuant to the previous order. As a result, the renewal application specifically stated that it did not seek [redacted] because the FBI had requested that information in a previous order but had not received it. Despite the fact that the renewal application did not seek and the court's order did not authorize production of [redacted] [redacted] company continued to provide the [redacted] after the renewal order was executed. (S)

b1

(S) The agent told the OIG that she did not know the [redacted] was being produced pursuant to the renewal order until approximately 2 months after the order was signed by the FISA Court. She said she first learned that the FBI had received [redacted] with respect to either order when an analyst in her field office informed her that the FBI was receiving [redacted] pursuant to, but not authorized by, the pen register/trap and trace order. After the analyst reported the matter to the agent, both NSLB and OIPR were informed. (S)

(S) The agent told us that the provider [redacted] [redacted] According to a technician, [redacted] [redacted]

(S) The FBI concluded that "information was improperly collected" and reported the incident to the IOB. The FBI also stated that the matter was reportable because records of [redacted] are statutorily protected. OIPR reported the incident to the FISA Court and provided the material that was not requested by the FBI or authorized by the FISA Court to the FISA Court for sequestration. (S)

An FBI Electronic Communication (EC) approved by the FBI Deputy General Counsel stated that the mistake was made by the provider and not the FBI. While we agree that the initial error was made by the provider, the FBI continued to receive and retain unauthorized information about a U.S. person for approximately 2 months. In this instance, the FBI continued to collect information about a U.S. person without review by the agent to ensure that it was authorized by the court order. (U)

(S) This case gave us concern that FBI agents may be unknowingly receiving in other cases [redacted] that has not been authorized by the FISA Court. We therefore interviewed each of the [redacted] agents who received combination orders for [redacted] in 2006. [redacted] said that they received cell site information as directed by the FISA Court. [redacted] other agents (including the agent in the matter described above) told us they did not know the FISA Court order had included a request for [redacted] [redacted] and they did not think they received it. One agent told us that he knew the information was requested, but that he thought he had to enforce the order in order to receive [redacted] ~~(S)~~

b1

(S) Because business records produced electronically pursuant to combination orders are not first reviewed by the agents before they are provided to FBI technicians, agents may be receiving [redacted] when it is not authorized and also may not realize that they have [redacted] [redacted] when it is authorized. Moreover, the FBI does not have procedures that require FBI agents or technicians to review business records (or pen register/trap and trace information) when they are first produced to ensure they have received only what is authorized by the FISA Court order. In addition, the FBI does not require agents to review court-ordered material before it is uploaded into FBI databases. ~~(S)~~

(S) This matter also illustrates the need for better communication between OIPR attorneys, NSLB attorneys, and FBI case agents. As noted above [redacted] agents told us that they were not aware that OIPR had attached a request for [redacted] to their pen register. Other agents we interviewed stated that they were not aware that OIPR or NSLB attorneys had added requests for subscriber information to their pen register/trap and trace requests. Our March 2007 Section 215 report also found that agents were not aware that OIPR added requests for subscriber information to their pen register/trap and trace requests. If agents do not know that

(S) ⁵¹ Our concern is not limited to the business record portion of the combination order, but also applies to pen register/trap and trace records when the records are [redacted]

(S) business record requests have been added. they will not know they should be or are receiving subscriber or [redacted] The lack of knowledge may contribute to IOB violations and the failure to identify IOB violations. In addition, agents may unnecessarily issue NSL for information previously ordered to be produced by the FISA Court.⁵² (S)

b1

B. Case 2 (U)

In response to a pure Section 215 order processed in 2006 and signed by the FISA Court in 2007, the FBI received information beyond the time period authorized by the order. (U)

The Section 215 order at issue required a company to produce records

(S) [redacted] The agent submitted the Section 215 request after the company refused to provide the business records on a voluntary basis. Although the order required the production of documents for a specified 5-month period, the company produced the records for 2 additional months. (S)

According to the FBI case agent, he realized that he received additional records beyond the scope of the FISA Court order a few days after he received the records. On October 2, 2007, the agent sent an EC to NSLB and the FBI Inspection Division reporting the matter as a potential IOB. The agent stated that he also reported the matter to OIPR. The agent told the OIG that he reviewed the records and created a copy of the data that did not include the 2 months of the unauthorized records. (U)

We discussed this matter with the FBI and OIPR. The FBI informed the OIG that it had determined that this matter was not reportable to the IOB. When we asked for documentation of this decision the FBI reported that it had none because it had determined that the incident should not have been reported to the NSLB as a potential IOB. We also asked whether the matter had been reported to the FISA Court. OIPR stated that it had not yet determined whether the matter was a compliance incident that should be reported to the FISA Court. (U)

⁵² We found another matter involving a combination order for pen register/trap and trace and subscriber information. The day after a FISA Court order expired, the provider continued its practice of faxing to the FBI agent a list of the phone numbers collected as a result of the surveillance order. The agent did not recall if he received subscriber information as required by the FISA Court order. Because we could not determine whether the fax included subscriber information, we did not include this matter in our analysis. (U)

(S) FBI officials stated that the FBI's receipt of 2 extra months of records is not reportable to the IOB because there is no statute prohibiting the company from voluntarily producing [redacted] to the FBI and thus the incident did not violate any statute, nor did it violate any Executive Order. The FBI stated that because there is no such violation, it should be able to treat the additional 2 months of records as a voluntary production independent of the FISA Court order. ~~(S)~~

b1

We disagree and believe that the production of these additional records should not be considered as voluntary and independent of the FISA Court order without further inquiry. First, the provider refused to produce any records to the FBI without a court order. Second, the FBI has chosen not to ask the provider whether the additional 2 months of records were produced inadvertently or voluntarily. Third, the collection includes information of U.S. persons who are not the subjects of any FBI national security investigation. Therefore, we believe that if the FBI wants to keep and use these records, it should either: (1) obtain written confirmation from the provider that the records were produced voluntarily, or (2) obtain a 215 order from the FISA Court for the production of the additional records. If the provider states that the production was not voluntary and the FISA Court declines to issue an additional order, the FBI should revisit its IOB determination and sequester the additional records with the FISA Court.⁵³
(U)

(S) FBI officials also suggested to us that they should be able to treat any non-statutorily protected records obtained pursuant to, but outside the scope of, a Section 215 order as a voluntary production of records independent of the order. We are troubled by this approach because [redacted]

⁵³ In its response to our report, the NSD stated that in both matters discussed in this Section "the FBI took the steps necessary to ensure that the over-produced information would not be used." However, this is only partially accurate. As discussed above, in Case 2 the agent initially isolated the additional material. However, the FBI later concluded that it should be able to use these additional records under the theory that they should be treated similar to materials that are voluntarily produced. We disagree with this analysis. Because of our concerns that the FBI should not use the material without either contacting the provider about the material or seeking an expanded FISA order, we made the recommendation discussed above. We look forward to the NSD's and FBI's specific response to that recommendation and how they intend to treat such material. (U)

(S)

[Redacted]

(S)

FBI officials expressed the view that [Redacted]

[Redacted]

[Redacted] However, we are concerned by the lack of any comprehensive policy memorializing this position and providing guidance to case agents.

~~(S)~~

In summary, we found two instances in which the FBI received more information than it had requested in response to Section 215 orders. In one case the FBI did not discover the incident for 2 months. [Redacted]

(S)

[Redacted]

[Redacted] The FBI reported the matter to the IOB, and OIPR reported the matter to and sequestered the material with the FISA Court. ~~(S)~~

In the other instance, the FBI quickly discovered the incident after the FBI had received the information from the provider. However, in this case, the FBI did not consider the matter to be reportable to the IOB because the records were not statutorily protected, and OIPR has not made a decision regarding whether this is a compliance incident reportable to the FISA Court. (U)

We recommend that the FBI develop procedures for reviewing materials received from Section 215 orders to ensure that it has not received information that is not authorized by the orders. (U)

Furthermore, we recommend that the FBI develop procedures for handling material that is produced in response to, but outside the scope of, a Section 215 order. The procedures should include the FBI's justification for handling any class of material provided in response to, but outside the scope of, a Section 215 order differently from other classes. We believe the FBI should not base the procedures for handling such material solely on whether the material is or is not statutorily protected. Instead, the procedures should also address such factors as whether the material contains non-public information about U.S. persons who are not the subjects of FBI national security investigations, and whether the underlying Section 215 order included particularized minimization procedures. In addition, these procedures should be incorporated in the minimization procedures required by the Reauthorization Act, a subject we discuss further in Chapter Seven. (U)

ACLU Sect. 215-1536

II. Other Noteworthy Items (U)

b1

(S) **A. Request for** [redacted]

(S) We considered the Section 215 request for [redacted] [redacted] discussed earlier in this report at pages 33 to 34 to be a noteworthy item. In this case, [redacted]

[redacted] However, the FBI subsequently issued NSLs for information [redacted] even though the statute authorizing the NSLs contained the same First Amendment restriction as Section 215 and the ECs authorizing the NSLs relied on the same facts contained in the Section 215 applications. We therefore describe this case in more detail in this section. ~~(S)~~

1. The FBI Investigation (U)

(S) [redacted]

(S) [redacted]

54 ~~(S)~~

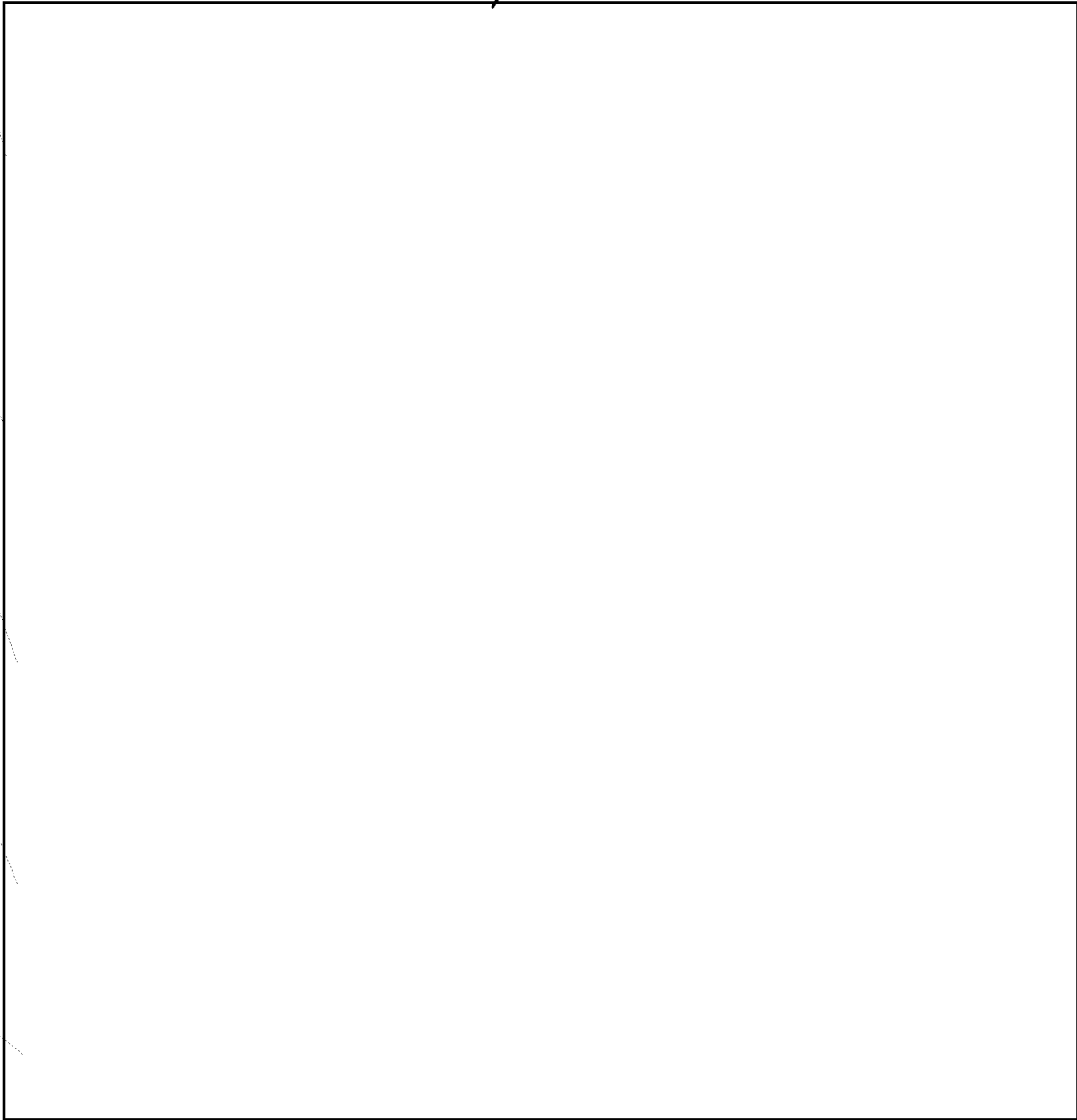
(S) [redacted]

55 ~~(S)~~

(S) 54 [redacted]

(S) 55 [redacted]

(S)



(S)

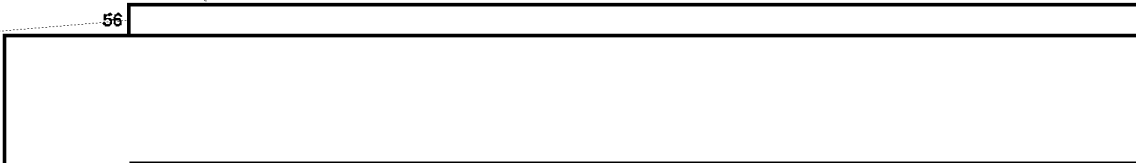
(S)

(S)

(S)

(S)

56



(S)

57



(S) [redacted] (S)

(S)

[redacted]

(S)

[redacted]

(S) When the FBI's Section 215 application was sent to OIPR for review, the assigned OIPR attorney initially raised First Amendment concerns with regard to the Section 215 application.⁵⁸ The NSLB attorney e-mailed the OIPR attorney on two occasions stating that she thought that the underlying FBI investigation [redacted] was legitimate. (S)

According to the OIPR attorney, OIPR attorneys had different views regarding how the First Amendment affected this Section 215 application and that these discussions delayed the submission of the application.⁵⁹ (U)

⁵⁸ Section 215 states that the FBI can apply for an order for the production of business records "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 of the Constitution." 50 U.S.C. § 1861(a)(1). (U)

⁵⁹ We asked the former Acting Counsel for Intelligence Policy how the First Amendment concerns were resolved, and she told us that the initial application was submitted after a meeting between the former Counsel of Intelligence Policy and the FBI General Counsel. However, neither the former Counsel for Intelligence Policy nor the FBI General Counsel said they recalled such a meeting. (U) ACLU Sect. 215-1539

2. The FISA Court's Objections to the Section 215 Application on First Amendment Grounds (U)

b1

(S)

(S)

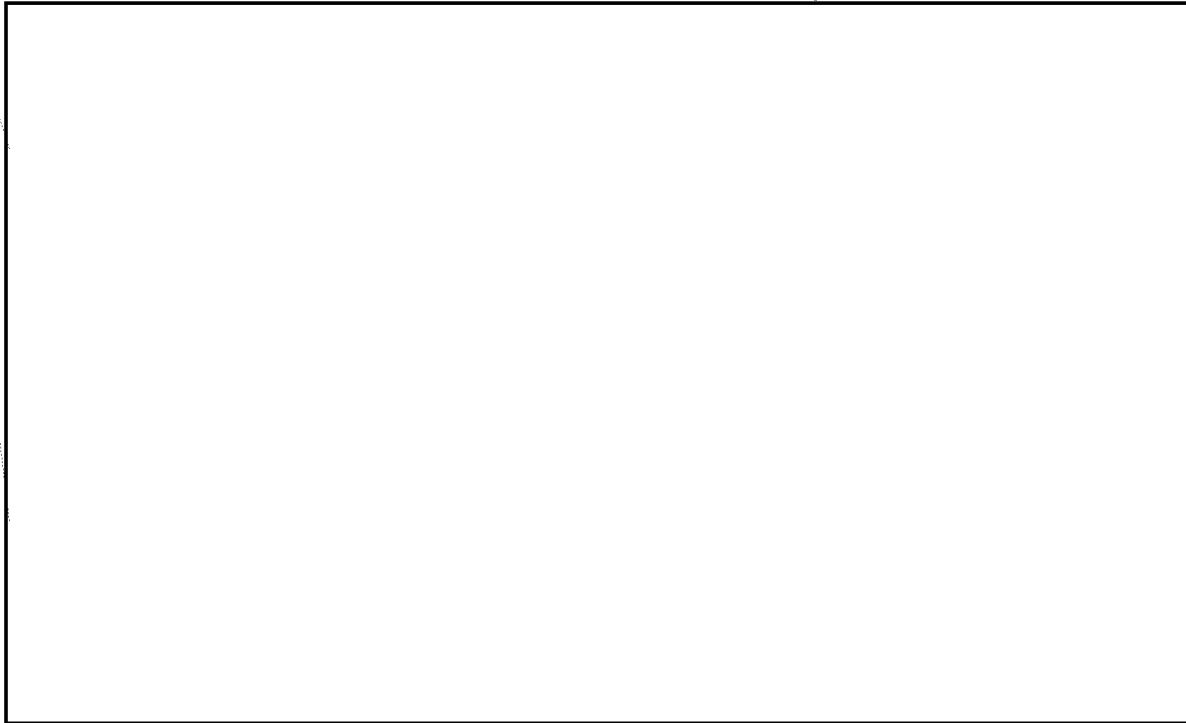


60 ~~(S)~~

The FISA Court declined to approve the first application. OIPR and NSLB e-mails state that the FISA Court decided that "the facts were too 'thin' and that this request implicated the target's First Amendment rights."
(U)

(S)

(S)



(S)

60



(S)

(S)

(S)

(S)

(S)

61

(S)

62

(S)



(S)

(S)

(S)

(S)

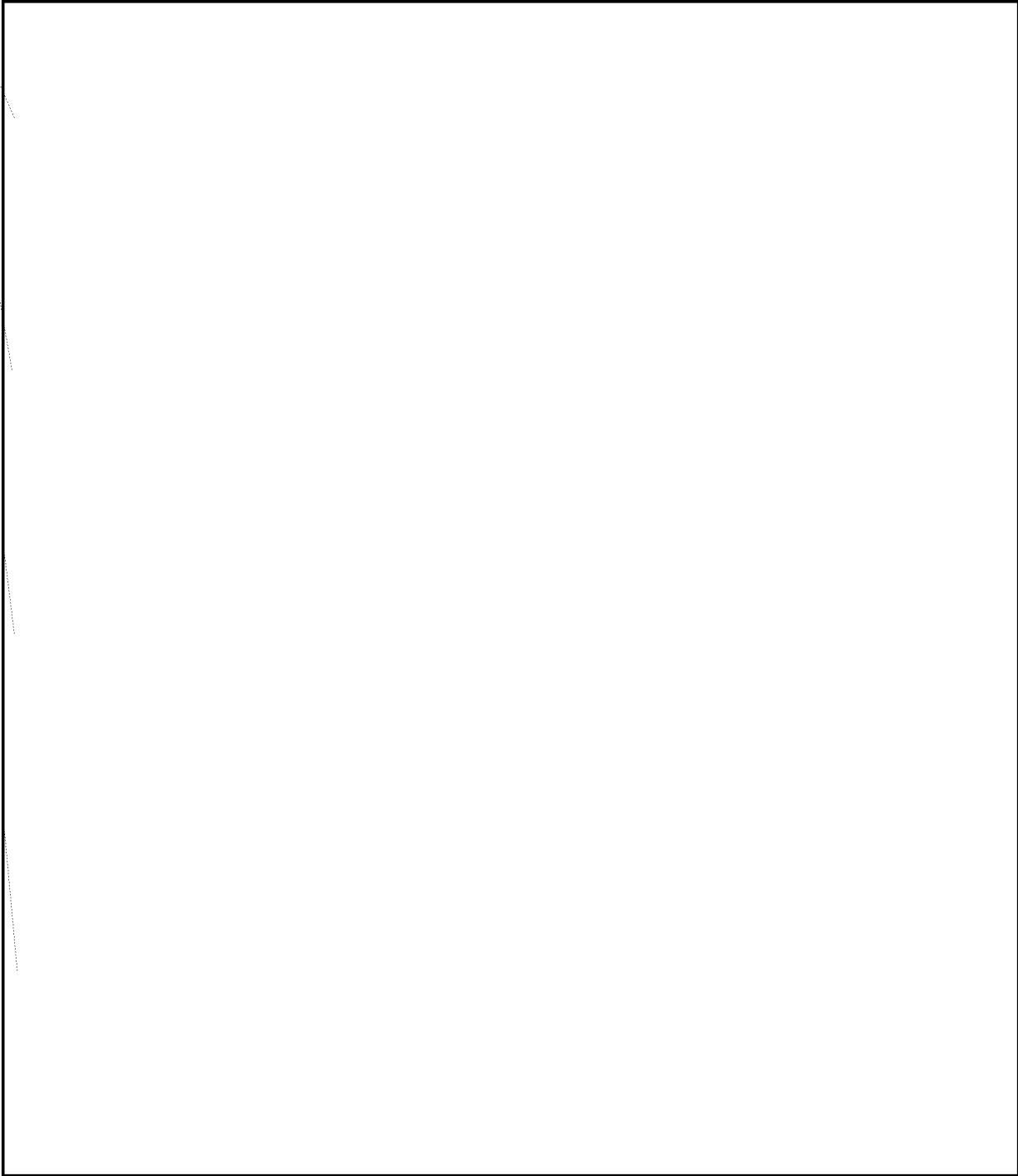
(S)

3. FBI and OIPR's Response (U)



(S)

(S)



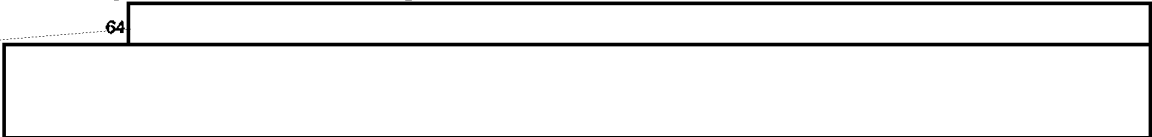
(S)

(S)

(S)

⁶³ The FBI General Counsel told the OIG that the FISA Court does not have the authority to close an FBI investigation. (U)

(S)



~~SECRET~~

We asked both the FBI General Counsel and the former Counsel for Intelligence Policy whether, in light of the Court's decision, they had reviewed the underlying investigation [redacted] to ensure that it was not being conducted in violation of the First Amendment caveat. The FBI General Counsel told us that she did not review the underlying investigation [redacted] because, for the reasons stated above, she believed there was enough information to predicate the investigation. She said she disagreed with the court and nothing in the court's ruling altered her belief that the investigation was appropriate. ~~(S)~~

b1

In contrast, the former Counsel for Intelligence Policy stated that OIPR should have examined the underlying investigation after the Court's decision regarding the Section 215 request. However, he said that with the increase in national security investigations and FISA requests, OIPR had not been able to fully serve such an oversight role.⁶⁵ (U)

In addition, the former Acting Counsel for Intelligence Policy stated that there is a history of significant pushback from the FBI when OIPR questions agents about the assertions included in FISA applications.⁶⁶ The OIPR attorney assigned to Section 215 requests also told us that she routinely accepts the FBI's assertions regarding the underlying investigations as fact and that the FBI would respond poorly if she questioned those assertions. (U)

We also asked the FBI General Counsel whether it was appropriate to issue NSLs in this investigation based on the same factual predicate as the Section 215 application given that the statutory provisions authorizing NSLs and Section 215 requests contain the same First Amendment caveat.⁶⁷ The FBI General Counsel told the OIG that she believed that it was appropriate to issue NSLs because she disagreed with the FISA Court and because the FBI was responsible for investigating [redacted] with other subjects of national security investigations. She stated that the FBI would

⁶⁵ According to the former Counsel for Intelligence Policy, he raised his concerns about OIPR's inability to fulfill its oversight role in late 2004 or early 2005. The former Acting Counsel for Intelligence Policy told us that, as of November 2007 OIPR developed a strategy for reviewing national security investigations and had begun conducting national security reviews. According to an OIPR attorney, OIPR has conducted all 15 of their planned national security reviews at approximately 14 field offices and FBI Headquarters. (U)

⁶⁶ The former Acting Counsel also stated that FBI agents are under significant pressure to respond to national security threats, and that some agents are angry that FBI agents have been accused of failing to identify these threats. (U)

⁶⁷ The FBI requested three NSLs [redacted] pursuant to the *Right to Financial Privacy Act* (RFPA), 12 U.S.C. § 3414. RFPA requires that the individual issuing the NSL certify that the investigation is "not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States." ~~(S)~~

ACLU Sect. 215-1544

72
~~SECRET~~

have to close numerous investigations if it was not permitted to investigate individuals based on their contact with other subjects of FBI investigations.

~~(S)~~

The former Counsel for Intelligence Policy stated that investigations based on association with subjects of other national security investigations are weak, but "are not necessarily illegitimate." He stated that when OIPR receives cases that appear to be based solely on association, OIPR first attempts to identify specific conduct by the subject and asks "what makes you - the FBI - think that this guy did anything wrong."

(S)

[Redacted]

b1

4. OIG Analysis (U)

We considered this matter to be noteworthy because the FISA Court twice refused to authorize Section 215 orders based on concerns that the investigation was premised on protected First Amendment activity, and the FBI subsequently issued NSLs to obtain information [Redacted] based on the same factual predicate without first reviewing the underlying investigation to ensure it did not violate the First Amendment caveat.

(S)

Section 215 allows the FBI to seek a business records order for a national security investigation of a U.S. person provided that the investigation is "not conducted solely upon the basis of activities protected by the first amendment of the Constitution." See 50 U.S.C. § 1861(a)(1) and (a)(2)(B). Similarly, the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414, allows the FBI to issue NSLs to obtain financial records for a national security investigation of a U.S. person provided that the investigation is "not conducted solely upon the basis of activities protected by the first amendment of the Constitution." (U)

In this matter, both FBI and OIPR personnel had raised First Amendment concerns regarding the predicate for the investigation [Redacted] before and after the first Section 215 read application was submitted to the FISA Court. Once the Court expressed similar concerns and rejected the successive applications, we believe it was incumbent upon the FBI and OIPR re-evaluate the investigation before seeking additional information about [Redacted] using NSLs. Instead, the FBI issued NSLs based on the same factual predicate contained in the Section 215 applications and without additional information about [Redacted] activities, despite the Court's rejection on two occasions of requests for a Section 215 order.

(S)

We were also concerned by [Redacted]

(S)

(S)

[Redacted]

b1

(S)

B. [Redacted] of Some Section 215 Requests ~~(S)~~

(S)

We also considered the [Redacted] of several Section 215 orders issued during 2006 to be a noteworthy item. [Redacted]

[Redacted]

(S)

[Redacted]

CHAPTER SEVEN MINIMIZATION PROCEDURES (U)

The Reauthorization Act required the Attorney General to adopt minimization procedures for business records obtained pursuant to Section 215 orders. 50 U.S.C. § 1861(g)(1). The Act also directed the OIG to examine the minimization procedures to determine whether they “protect the constitutional rights of United States persons.” See Pub. L. No. 109-177, § 106A. In this chapter, we describe our review of the minimization procedures adopted by the Department. (U)

I. Minimization Mandate (U)

The Reauthorization Act defined minimization procedures as: (U)

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the 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;⁶⁸ (U)

(B) procedures that require that non-publicly 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

⁶⁸ Foreign Intelligence information is defined as:

(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 or 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(e). (U)

ACLU Sect. 215-1547

identity is necessary to understand foreign intelligence information or assess its importance; and (U)

(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. 50 U.S.C § 1861(g)(2). (U)

The minimization procedures were required to be adopted by the Attorney General within 180 days of enactment of the Reauthorization Act (that is, by September 5, 2006). 50 U.S.C § 1861(g)(1). (U)

As noted above, the Act also required that the OIG examine "the minimization procedures adopted by the Attorney General . . . and whether such minimization procedures protect the constitutional rights of United States persons." (U)

II. Draft Minimization Procedures (U)

Several months after enactment of the Reauthorization Act, the Office of Intelligence Policy and Review (OIPR) and the FBI – both of whom had been developing minimization procedures related to Section 215 orders – exchanged draft procedures. The drafts differed in fundamental respects, ranging from definitions to the scope of the procedures. At a meeting held on August 21, 2006, approximately 2 weeks before the statutory deadline, FBI and OIPR officials were unable to reach agreement on minimization procedures. Present at the meeting were the FBI General Counsel and the former Counsel for Intelligence Policy, along with attorneys from their respective offices and representatives from the Deputy Attorney General's Office, the Criminal Division, the Office of the Director of National Intelligence, and the Central Intelligence Agency. (U)

Unresolved issues included the time period for retention of information, definitional issues of "U.S. person identifying information," and whether to include procedures for addressing material received in response to, but beyond the scope of, the FISA Court order; uploading information into FBI databases; and handling large or sensitive data collections. (U)

For example, the Reauthorization Act calls for minimization procedures that prohibit the dissemination of non-public U.S. person information in a manner that would identify the U.S. person in certain circumstances. However, OIPR and the FBI could not agree on a definition of "U.S. person identifying information." [REDACTED]

(S)

b1

(S)

[Redacted]

In addition, OIPR and the FBI could not agree on the time period for retention of business records obtained by Section 215 orders.

(S)

[Redacted]

(S)

[Redacted]

(S)

(S)

ACLU Sect. 215-1549

(S)



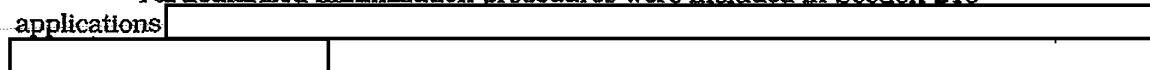
In an effort to meet the statutory deadline after the August 21 meeting the former Counsel for Intelligence Policy suggested that the Attorney General adopt sections of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collections of October 31, 2003, (NSI Guidelines) as interim minimization procedures. According to OIPR and FBI attorneys, the suggestion was adopted for several reasons. First, it allowed the Attorney General to meet the statutory deadline. Second, compliance with the NSI Guidelines in their entirety was already a prerequisite to obtaining a Section 215 order. Third, the suggestion allowed the parties to continue efforts to resolve their differences in other forums. (U)

During this period the FBI and OIPR also were discussing some of the same issues with respect to updating the minimization procedures for full FISA orders. FBI and OIPR attorneys told us that they believed that the minimization procedures for full FISA orders could supersede or at least serve as a model for the minimization procedures for Section 215 business records since the discussions regarding full FISA orders required the resolution of broader and more complex issues.⁷⁰ (U)

In addition, the Office of the Director of National Intelligence convened a working group composed of representatives from the intelligence community to discuss, among other things, the lack of consistency in their guidelines for national security investigations and the need to develop common definitions for terms including "U.S. person identifying information."⁷¹ (U)

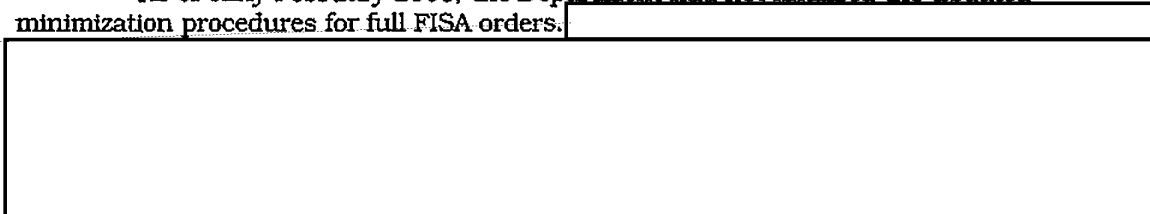
⁶⁹ Particularized minimization procedures were included in Section 215 applications

(S)



⁷⁰ As of early February 2008, the Department had not finalized the updated minimization procedures for full FISA orders.

(S)



⁷¹ As of early December 2007, the working group had not defined "U.S. person identifying information." (U)

III. The Interim Standard Minimization Procedures (U)

On September 5, 2006, the Attorney General signed the Interim Standard Minimization Procedures (Interim Procedures) and filed the procedures with the FISA Court. The Interim Procedures adopted four sections of the NSI Guidelines and stated that the sections are to be "construed" to meet the statutory definitions of minimization procedures contained in the Reauthorization Act. (U)

The four sections of the NSI Guidelines included in the Interim Procedures are: (1) Respect for Legal Rights; (2) Determination of United States Person Status; (3) Retention and Dissemination of Information; and (4) Definitions.⁷² (U)

The Respect for Legal Rights section states that the NSI Guidelines do not authorize investigating or maintaining U.S. person information solely for the purpose of monitoring protected First Amendment activities or the lawful exercise of Constitutional or statutory rights. In addition, this section requires that investigations be conducted in conformity with applicable authorities including the Constitution, statutes, executive orders, Department regulations and policies, and Attorney General Guidelines. (U)

The Determination of United States Person Status section defines a "United States Person" as including U.S. citizens and aliens lawfully admitted for permanent residence. The section also provides guidance in determining a person's status [redacted]

b1

(S)

The Retention and Dissemination of Information section contains three subsections: Information Systems and Databases; Information Sharing; and Special Statutory Requirements. The Interim Standard Minimization Procedures adopt only the first and second sections.⁷³ (U)

The Information Systems and Databases subsection requires that the FBI retain records of investigations in accordance with a plan approved by the National Archives and provides for OIPR oversight of information obtained in the course of a national security investigation. (U)

⁷² See, respectively, NSI Guidelines Parts I.B.3; I.C; VII.A.1 and B; and VII. (U)

⁷³ The Special Statutory Requirements section requires that FISA-derived information be disseminated pursuant to the minimization procedures approved by the FISA Court and as specified in the FISA statute. Although not formally adopted in the Interim Standard Minimization Procedures, this section - as with every section in the NSI Guidelines - governs the use of Section 215 derived information because compliance with the NSI Guidelines in their entirety is already a prerequisite to obtaining a Section 215 order. (U)

~~SECRET~~

The Information Sharing subsection identifies the Department's policy to share information with relevant agencies unless there is a specific provision limiting such information sharing. To that end, the section provides that the FBI may disseminate information within the Department, with other federal, state, and local entities, and with foreign authorities when the information relates to the recipient's authorized responsibilities and is consistent with national security interests. (U)

The Definition section of the NSI Guidelines defines terms such as "foreign intelligence," "international terrorism," and "publicly available." However, the Guidelines do not define "U.S. person identifying information." (U)

We asked FBI and OIPR officials whether they believed the interim procedures met the minimization requirements of the Reauthorization Act. We specifically inquired whether the interim procedures could meet the statutory requirements when adherence to the NSI Guidelines was already a statutory requirement for obtaining a Section 215 order, the NSI Guidelines were not specific, and the NSI Guidelines applied to all documents the FBI collected in the course of a national security investigation and were not "designed in light of the purpose and technique" of Section 215 requests, as required by the Reauthorization Act. (U)

OIPR and FBI attorneys responded that they believed the interim procedures met the statutory requirement because the Reauthorization Act did not require that the minimization procedures be "new" or "in addition to" existing requirements. (U)

When we asked how an agent would determine, for example, whether the disclosure of U.S. person identifying information is necessary to understand foreign intelligence or assess its importance, the FBI General Counsel stated that the determination must be made on a case-by-case basis. The former Counsel for Intelligence Policy stated that pursuant to the interim procedures the FBI employee disseminating the information would make a judgment call. The former Counsel for Intelligence Policy also noted that this was one of the unresolved issues and that he hoped these issues would be addressed as the FBI and OIPR updated the minimization procedures for full FISA orders. (U)

We also asked the FBI whether the retention plan approved by the National Archives required FBI agents to examine records received pursuant to a Section 215 order upon receipt to ensure compliance with the order. As discussed previously, we believe such a requirement could prevent the retention of U.S. person information that was produced pursuant to but not authorized by a Section 215 order. However, we were told that the FBI does not have a current retention policy for counterterrorism cases and until such a policy is developed, the FBI will rely on a default retention policy which addresses only the duration of retention and does not address the

80
~~SECRET~~

ACLU Sect. 215-1552

(S) need to review the material. According to the FBI's default retention policy for counterterrorism cases, the FBI will retain information obtained during a national security investigation for [redacted] before the issue of further retention is re-evaluated. (S)

IV. OIG ANALYSIS (U)

As discussed above, because of a series of disagreements about how the FBI should retain and disseminate business records obtained pursuant to a Section 215 order, in September 2006 the Department issued "interim" minimization procedures for business records produced pursuant to Section 215 orders. These interim minimization procedures use general hortatory language stating that all activities conducted in relation to national security investigations must be "carried out in conformity with the Constitution." However, we believe this broad standard does not provide the specific guidance for minimization procedures that the Reauthorization Act appears to contemplate. (U)

When discussing the issue raised by the Reauthorization Act of whether the minimization procedures "protect the constitutional rights of United States persons," OIPR and FBI attorneys asserted that most government requests for business records do not raise constitutional concerns. They noted that the Supreme Court has held that individuals have no legitimate expectation of privacy for information voluntarily turned over to third parties. See e.g., *United States v. Miller*, 425 U.S. 435, 442-444 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979); *Couch v. United States*, 409 U.S. 332, 335-336 (1973). Yet, not every business record obtainable through a Section 215 order falls under this rubric. For example, a request by the government for business records created and maintained by a sole proprietor may raise Fifth Amendment concerns. *Bellis v. United States*, 417 U.S. 85 (1974).⁷⁴ Business record requests also may affect First Amendment rights of individuals. In addition, the Supreme Court also has not ruled on the appropriate privacy interest to be afforded to [redacted]

Moreover, the Reauthorization Act required the Department to adopt "specific procedures" reasonably designed "to minimize the 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." We believe that the interim procedures do not adequately address this

(S) 74 [redacted]

requirement, and we recommend that the Department continue its efforts to construct specific minimization procedures relating to Section 215 orders, rather than rely on general language in the Attorney General's NSI Guidelines. (U)

First, the interim procedures do not provide specific guidance regarding the retention of U.S. person information. The FBI acknowledged that its practice under the NSI Guidelines sections is to retain all information obtained in the course of a national security investigation for a period [redacted] However, the Reauthorization Act requires the Department to adopt "specific procedures" designed to minimize the retention 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. The Department's failure to distinguish the retention of U.S. person information from any other information obtained in the course of national security investigations appears inconsistent with the language of the Reauthorization Act. Moreover, while OIPR proposed retaining the business records [redacted] and the FBI recommended retaining them [redacted] the interim guidelines simply follow general archives practices and allow the information to be retained without further evaluation [redacted]

b1

Similarly, the interim procedures do not contain procedures that prohibit the dissemination of U.S. person information unless disclosure is necessary to understand or address the importance of the intelligence information. The FBI's assertion that agents can make this determination on a case-by-case basis conflicts with the statutory requirements that specific minimization procedures be developed to address this concern. (U)

[redacted]

[redacted] ignores the Reauthorization Act's statutory requirement that the Department adopt procedures "that are reasonably designed in light of the purpose and technique" of business records orders to minimize the retention and prohibit the dissemination of U.S. person information." We believe that standard procedures should be specifically adopted [redacted] in accord with the requirements and intent of the Reauthorization Act.⁷⁵ ~~(S)~~

[redacted]

~~SECRET~~

As a result, we recommend that the FBI and OIPR continue to work to develop appropriate standard minimization procedures for business records. Pursuant to the Reauthorization Act, the Department should replace the interim procedures with final standard minimization procedures that provide specific guidance for the retention and dissemination of U.S. person information. In addition, we recommend that the FBI and OIPR monitor Section 215 requests to ensure that if a request implicates the rights of U.S. persons, that specific and particularized minimization procedures be included in the Section 215 application and implemented in a manner that protects the U.S. person's constitutional rights. (U)

(S)



b1

83
~~SECRET~~

ACLU Sect. 215-1555

CHAPTER EIGHT CONCLUSIONS (U)

As required by the Reauthorization Act, the OIG conducted this review of the FBI's use of Section 215 requests for business records in 2006. The Reauthorization Act required the OIG to examine how many requests were prepared by the FBI; how many applications were approved, denied, or modified by the Foreign Intelligence Surveillance Act (FISA) Court; whether bureaucratic or other impediments hindered the FBI's use of Section 215; and the effectiveness of the FBI's use of Section 215. The Act also directed that the OIG examine any improper use of Section 215 authority and identify any noteworthy facts or circumstances concerning Section 215 requests. Finally, the Act required the OIG to examine whether the minimization procedures adopted by the Department protect the constitutional rights of U.S. persons. As required by the Reauthorization Act, our review covered Section 215 requests processed in calendar year 2006. (U)

We found that in 2006 the FBI and OIPR processed a total of 21 pure Section 215 applications and 32 combination applications. All but six of the pure Section 215 applications were formally submitted to the FISA Court. Each of the 47 Section 215 applications (15 pure requests and 32 combination requests) formally submitted to the FISA Court were approved.⁷⁶ (U)

The six pure Section 215 requests that were not formally presented to the FISA Court were withdrawn either while they were pending approval at the FBI's National Security Law Branch (NSLB) or at the Office of Intelligence and Policy Review (OIPR) because they lacked sufficient predicate or the provider did not maintain the records requested. The FBI obtained a wide variety of records using Section 215 orders in 2006, including credit card records, [REDACTED]

(S)

b1

[REDACTED]

(S)

Unlike in previous years, [REDACTED]

[REDACTED]

⁷⁶ Four of the pure Section 215 applications processed in 2006 were signed by the FISA Court in 2007. (U)

We determined that when FBI agents submitted Section 215 requests processed in 2006, they encountered similar processing delays as those identified in our March 2007 report. These delays were caused by unfamiliarity with Section 215 orders, too few resources to handle requests expeditiously, the multi-layered review process, and substantive issues regarding whether the application met the statutory requirements. Overall, the average processing time for Section 215 orders in 2006 was 147 days, which was similar to the processing time for 2005. However, the FBI and OIPR were able to expedite certain Section 215 requests in 2006, and when the FBI identified two emergency requests the FBI and OIPR processed both Section 215 requests quickly. (U)

We uncovered no evidence of harm to national security in any specific cases caused by the delay in obtaining Section 215 orders or by the FBI's inability to obtain information that was requested in Section 215 requests. However, agents expressed frustration about the amount of time and effort involved in obtaining a Section 215 order and stated that they would first pursue the information through other more efficient investigative techniques such as voluntary compliance and national security letters. (U)

We again examined how the FBI in 2006 used information obtained through Section 215 orders in national security investigations. Aside from

(S)

[redacted]
Section 215 orders were used primarily to exhaust investigative leads, although in some instances the FBI obtained information to support additional FBI investigative requests and to [redacted]

b1

[redacted] The evidence showed no instance where the information obtained from a Section 215 order described in the body of the report resulted in a major investigative development. However, [redacted]
[redacted]

We did not identify any illegal use of Section 215 authority. However, we identified two instances where the FBI received information inadvertently that was not authorized by the FISA Court order. In one instance, the FBI did not realize for 2 months that it was continuously receiving information that was not authorized by the FISA Court order. The FBI reported this matter to the IOB, and OIPR reported the matter to and sequestered the material with the FISA Court. (U)

In the other instance the FBI recognized the matter quickly and took steps to immediately sequester the additional material. However, in this case, the FBI did not consider the matter to be reportable to the IOB because the records were not statutorily protected. OIPR has not made a decision regarding whether this is a compliance incident reportable to the FISA Court. (U)

ACLU Sect. 215-1557

We recommend the FBI should develop procedures that require FBI employees to review materials received from Section 215 orders to ensure that the material they receive pursuant to a Section 215 is authorized by the Section 215 order. (U)

Furthermore, we recommend that the FBI develop procedures for identifying and handling material that is produced pursuant to, but outside the scope of, Section 215 orders. The procedures should include the FBI's justification for handling any class of such material differently from other classes and should consider factors in addition to whether the material is or is not statutorily protected. For example, the procedures should also address such factors as whether the material contains non-public information about U.S. persons who are not the subjects of FBI national security investigations, and whether the underlying Section 215 order included particularized minimization procedures. These procedures should be incorporated in the minimization procedures required by the Reauthorization Act. (U)

We identified two other "noteworthy" items. The first involved a

(S)

request

[Redacted]

b1

The second noteworthy item concerned the

(S)

[Redacted]

Finally, we examined whether the interim standard minimization procedures adopted by the Department for Section 215 orders are consistent with the requirements of the Reauthorization Act. Because of differences between the FBI and OIPR, the Department's interim procedures merely adopt the general language contained in the Attorney General's National Security Guidelines. However, these general standards do not provide specific guidance for minimization procedures that the Reauthorization Act appears to contemplate. We believe that these interim

~~SECRET~~

guidelines do not adequately address the intent and requirements of the Reauthorization Act for minimization procedures, and we recommend that the Department continue its efforts to develop specific standard minimization procedures relating to Section 215 orders. (U)

ACLU Sect. 215-1559.

87
~~SECRET~~

UNCLASSIFIED APPENDIX

UNCLASSIFIED

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

MAR 07 2008

The Honorable Glenn A. Fine
Inspector General
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Mr. Fine:

(U) Thank you for providing us a copy of your draft report dated January 28, 2008 titled, "A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records in 2006." We have also reviewed the subsequent draft provided to us on February 19. We appreciate the opportunity to comment, and note that this comment addresses the draft dated February 19, 2008.

(U) As you note in your report, Section 215 orders are an invaluable tool the Federal Bureau of Investigation uses to obtain information in national security investigations. In many cases, the information obtained through this investigative technique cannot be obtained by other means. We thank you for the extensive review your office has conducted of the use of this authority.

Sincerely,



J.M. McConnell

ACLU Sect. 215-1561

UNCLASSIFIED



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

March 3, 2008

The Honorable Glenn A. Fine
Inspector General
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Fine:

Thank you for the opportunity to respond to your report entitled, "A Review of the Federal Bureau of Investigation's use of Section 215 Orders for Business Records in 2006." We are pleased that your report recognizes the importance of this valuable tool to the Federal Bureau of Investigation's (FBI) conduct of national security investigations.

As you find in your report, FBI agents depend on Section 215 orders to support FBI national security investigations and to follow through on investigative leads. The process for obtaining these orders was designed to protect the privacy and civil liberties of Americans and to ensure that applications comply with statutory requirements. We appreciate your finding that this careful, measured approach—while resulting in some delay—has not caused any harm to the national security. In order to help ensure that the Department takes full advantage of this important tool in the future, the National Security Division (NSD) has augmented the number of attorneys handling Section 215 applications, and is collaborating with the FBI to increase the efficiency with which requests for Section 215 authority are prepared. Indeed, as you note, the FBI and the NSD were able to work together to obtain Section 215 authority expeditiously in 2006 when circumstances required immediate collection.

Your report also discusses the interim minimization procedures adopted by the Attorney General to govern Section 215 requests. As you note, at the time these procedures were adopted, the Department was in the process of revising its standard minimization procedures for other types of FISA collection. To allow Department attorneys the time to produce Section 215 minimization procedures consistent with that revision while ensuring that Americans' privacy and civil liberties interests are protected, the current interim procedures were adopted. The Interim Standard Minimization Procedures apply the requirements of four sections of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collections (October 31, 2003) to records obtained pursuant to Section 215. Since their adoption, the Foreign Intelligence Surveillance Court (FISC) has ordered the government to follow these minimization procedures in numerous Section 215 orders. With the revision of the procedures for other FISA collections now complete, the Department will commence work to

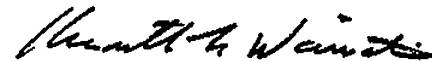
ACLU Sect. 215-1562

replace these interim procedures with standard minimization procedures specifically tailored to collection under Section 215.

Finally, we are pleased that your report confirms there were no illegal uses of Section 215 authority in 2006. Your report does note two instances in which a third party over-produced certain records in response to a court-authorized Section 215 request. As you discuss in your report, the FBI did not solicit the additional business records in either case and therefore cannot be faulted for the recipients' production of records beyond the scope of the court order. Indeed, in both instances you identify, the FBI took the steps necessary to ensure that the over-produced information would not be used.

Thank you for your efforts and for the opportunity to convey our comments on this report.

Sincerely,



Kenneth L. Wainstein
Assistant Attorney General



U.S. Department of Justice

Federal Bureau of Investigation

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 03-23-2012 BY 65179 DMH/STP/MJS

Office of the Director

Washington, D.C. 20535

March 5, 2008

Honorable Glenn Fine
Inspector General
United States Department of Justice
950 Pennsylvania Ave. N.W, Suite 4706
Washington, D.C. 20530

Re: Office of Inspector General Report: A Review of the
Federal Bureau of Investigation's Use of Section 215 Orders

Dear Mr. Fine:

The FBI appreciates this opportunity to respond to the findings and recommendations made in a "A Review of the Federal Bureau of Investigation's Use of Section 215 Orders" (215 Report), a report that was Congressionally mandated by the USA PATRIOT Improvement and Reauthorization Act of 2005. This letter conveys the FBI's response to the findings and recommendations of the Report, and I request that it be appended to the Report.

We are pleased that your office has concluded that the FBI did not engage in any illegal use of its authority to gather third party business records during national security investigations. We also appreciate your findings, with which we concur, that "Section 215 can be a valuable investigative tool" even though delays in obtaining such orders have, at times, undercut that value. Finally, we appreciate your conclusion that emergency requests were handled very quickly and that the average processing time for business record applications was reduced slightly during 2006 as compared to 2004 and 2005 because "FBI and OIPR attorneys developed a procedure and working relationship that allowed them to process business records orders more efficiently." We are hopeful these processing times will continue to fall in the coming years.

Thank you for the opportunity to respond to the report.

Very truly yours,

Robert S. Mueller, III
Director

ACLU Sect. 215-1564

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

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

Total Deleted Page(s) ~ 24
Page 2 ~ Outside the Scope
Page 3 ~ Outside the Scope
Page 4 ~ Outside the Scope
Page 5 ~ Outside the Scope
Page 6 ~ Outside the Scope
Page 14 ~ b7E
Page 15 ~ b7E
Page 16 ~ b7E
Page 17 ~ b7E
Page 18 ~ b1, b7E
Page 19 ~ b1, b7E
Page 20 ~ b1, b7E
Page 21 ~ b1, b7E
Page 22 ~ b1, b7E
Page 23 ~ b1, b7E
Page 67 ~ b6, b7C, b7E
Page 68 ~ b7E
Page 69 ~ b6, b7C, b7E
Page 70 ~ b6, b7C, b7E
Page 79 ~ Duplicate
Page 80 ~ Duplicate
Page 81 ~ Duplicate
Page 82 ~ Duplicate
Page 83 ~ Duplicate