EXECUTIVE SUMMARY

In the USA PATRIOT Improvement and Reauthorization Act of 2005 (Patriot Reauthorization Act), Congress directed the Department of Justice (Department) Office of the Inspector General (OIG) to review "the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice." See Pub. L. No. 109-177, § 119. Four federal statutes contain five specific provisions authorizing the Federal Bureau of Investigation (FBI) to issue national security letters (NSLs) to obtain information from third parties, such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies. In these letters, the FBI can direct third parties to provide customer account information and transactional records, such as telephone toll billing records.

Congress directed the OIG to review the use of NSLs for two time periods – calendar years (CY) 2003 through 2004 and CY 2005 through 2006. The first report is due to Congress on March 9, 2007; the second is due on December 31, 2007.[1] Although we were only required to review calendar years 2003 and 2004 in the first review, we elected to include data from calendar year 2005 as well.

In the Patriot Reauthorization Act, Congress directed the OIG's review to include:

(1) an examination of the use of national security letters by the Department of Justice during calendar years 2003 through 2006;

(2) a description of any noteworthy facts or circumstances relating to such use, including any improper or illegal use of such authority; and

(3) an examination of the effectiveness of national security letters as an investigative tool, including –

---

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

[1] The Patriot Reauthorization Act also directed the OIG to conduct reviews for the same two time periods on the use and effectiveness of Section 215 of the Patriot Act, a new authority under the Patriot Act that authorizes the FBI to obtain business record orders from the Foreign Intelligence Surveillance Court. The OIG's first report on the use and effectiveness of Section 215 orders is contained in a separate report issued in conjunction with this review of NSLs.

(A) the importance of the information acquired by the Department of Justice to the intelligence activities of the Department of Justice or to any other department or agency of the Federal Government;

(B) the manner in which such information is collected, retained, analyzed, and disseminated by the Department of Justice, including any direct access to such information (such as access to "raw data") provided to any other department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;

(C) whether, and how often, the Department of Justice utilized such information to produce an analytical intelligence product for distribution within the Department of Justice, to the intelligence community . . ., or to other Federal, State, local, or tribal government departments, agencies or instrumentalities;

(D) whether, and how often, the Department of Justice provided such information to law enforcement authorities for use in criminal proceedings . . . .[2]

In this report, we address each of these issues. To examine these issues, the OIG conducted interviews of over 100 FBI employees, including personnel at FBI Headquarters and at the Department. OIG teams also traveled to FBI field offices in New York, Chicago, Philadelphia, and San Francisco where we interviewed over 50 FBI employees. In the field offices, the OIG teams examined a judgmental sample of 77 counterterrorism and counterintelligence investigative cases files and 293 NSLs issued by those field offices to determine if the NSLs complied with relevant statutes, Attorney General Guidelines, and internal FBI policy.

The OIG also analyzed the FBI's NSL tracking database maintained by the FBI's Office of the General Counsel (FBI-OGC), which is the only database that compiles information on NSL usage for the entire FBI. The OGC database is used by the FBI to collect information that the Department is required to report to Congress in semiannual classified reports and, since passage of the Patriot Reauthorization Act, in an annual public report. We performed various tests on the OGC database to assess the accuracy and reliability of the FBI's reports.

---

[2] Patriot Reauthorization Act § 119(b).

This Executive Summary summarizes our full 126-page report of investigation on NSLs, including its main findings, conclusions, and recommendations.

The Appendix to the report contains comments on the report by the Attorney General, the Director of National Intelligence, and the FBI. The Appendix also contains copies of the national security letter statutes in effect prior to the Patriot Reauthorization Act. The classified report also contains a classified appendix.

I. Background on National Security Letters

The Patriot Act significantly expanded the FBI's preexisting authority to obtain information through national security letters.[3] Section 505 of the Patriot Act broadened the FBI's authority by eliminating the requirement that the information sought in an NSL must pertain to a foreign power or an agent of a foreign power. This section of the Patriot Act statute substituted the lower threshold that the information sought must be relevant to an investigation to protect against international terrorism or espionage, provided that the investigation of a United States person is not conducted "solely on the basis of activities protected by the first amendment of the Constitution of the United States." As a consequence of this lower threshold, NSLs may request information about persons other than the subjects of FBI national security investigations so long as the requested information is relevant to an authorized investigation.

Section 505 of the Patriot Act also permits Special Agents in Charge of the FBI's 56 field offices to sign NSLs, a change that significantly expanded approval authority beyond the pre-Patriot Act group of senior FBI Headquarters officials authorized to sign NSLs.

In addition, the Patriot Act added a new authority permitting the FBI to use NSLs to obtain consumer full credit reports in international terrorism investigations pursuant to an amendment to the Fair Credit Reporting Act (FCRA).[4]

NSLs may be issued by the FBI in the course of national security investigations, which are governed by Attorney General Guidelines.[5] The

---

[3] 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."

[4] 15 U.S.C. § 1681v (Supp. IV 2005).

[5] During the time period covered by this review, calendar years 2003 through 2005, the Attorney General Guidelines for national security investigations were revised. From January 1, 2003, through October 31, 2003, investigations of international terrorism or espionage were governed by the Attorney General Guidelines for FBI Foreign Intelligence

Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) authorize the FBI to conduct investigations concerning threats or potential threats to the national security, including threats arising from international terrorism, espionage, other intelligence activities, and foreign computer intrusions. The NSI Guidelines authorize three levels of investigative activity – threat assessments, preliminary investigations, and full investigations. NSLs are among the investigative techniques that are permitted to be used during national security investigations.

A. The Four National Security Letter Statutes

There are four statutes authorizing the FBI to issue five types of NSLs. We discuss each of these statutes below:

1. The Right to Financial Privacy Act

The Right to Financial Privacy Act (RFPA) was enacted in 1978 "to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity."[6] The RFPA requires federal government agencies to provide individuals with advance notice of requested disclosures of personal financial information and affords individuals an opportunity to challenge the request before disclosure is made to law enforcement authorities.[7]

The RFPA NSL statute, enacted in 1986, created an exception to the advance notice requirement that permitted the FBI to obtain financial institution records in foreign counterintelligence cases. Since the Patriot Act, the FBI may obtain financial records upon certification that the information is sought.

> for foreign counterintelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.[8]

(cont'd.)

Collection and Foreign Counterintelligence Investigations (FCI Guidelines)(March 1999). Effective October 31, 2003, these investigations were conducted pursuant to the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines).

[6] H.R. Rep. No. 95-1383, at 33 (1978).

[7] 12 U.S.C. §§ 3401-3422 (2000).

[8] 12 U.S.C. § 3414(a)(5)(A) (2000 & Supp. IV 2005).

The types of financial information the FBI can obtain through RFPA national security letters include information concerning open and closed checking and savings accounts and safe deposit box records from banks, credit unions, thrift institutions, investment banks or investment companies, as well as transactions with issuers of travelers checks, operators of credit card systems, pawnbrokers, loan or finance companies, travel agencies, real estate companies, casinos, and other entities.

2. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA), enacted in 1986, extends statutory protection to electronic and wire communications stored by third parties, such as telephone companies and Internet service providers.[9]

The ECPA NSL statute allows the FBI to obtain "subscriber information and toll billing records information, or electronic communication transactional records" from a "wire or electronic communications service provider" in conjunction with a foreign counterintelligence investigation upon certification that the information sought is

> relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities provided that such an investigation of a United States person is not conducted solely on the basis on activities protected by the first amendment to the Constitution of the United States.[10]

The types of telephone and e-mail transactional information the FBI can obtain through ECPA national security letters include:

- Historical information on telephone calls made and received from a specified number, including land lines, cellular phones, prepaid phone card calls, toll free calls, alternate billed number calls (calls billed to third parties), and local and long distance billing records associated with the phone numbers (known as toll records);
- Electronic communication transactional records (e-mails), including e-mail addresses associated with the account; screen names; and billing records and method of payment; and

---

[9] 18 U.S.C. § 2709 (1988).

[10] 18 U.S.C. § 2709(b)(2) (2000 & Supp. IV 2005).

- Subscriber information associated with particular telephone numbers or e-mail addresses, such as the name, address, length of service, and method of payment.[11]

3. The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) was enacted in 1970 to protect personal information collected by credit reporting agencies.[12] As amended by the Patriot Act, the FCRA authorizes two types of national security letters, FCRAu and FCRAv NSLs. The initial FCRA NSL statute, enacted in 1996, authorizes the FBI and certain other government agencies to issue NSLs to obtain a limited amount of information about an individual's credit history: the names and addresses of all financial institutions at which a consumer maintains or has maintained an account; and consumer identifying information limited to name, current address, former addresses, places of employment, or former places of employment pursuant to FCRAu NSLs.[13] Since the Patriot Act, the certifying official must certify that the information requested is

> sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.[14]

In 2001, the Patriot Act amended the FCRA to add a new national security letter authority, referred to as FCRAv NSLs, which authorizes the FBI to obtain a consumer reporting agency's credit reports and "all other" consumer information in its files.[15] Thus, since the Patriot Act, the FBI can now obtain full credit reports on individuals during national security investigations. The certifying official must certify that the information is "necessary for" the FBI's "investigations of, or intelligence or counter-intelligence activities or analysis related to, international terrorism . . . ."[16]

---

[11] The ECPA permits access only to "subscriber and toll billing records information" or "electronic communication transactional records," as distinguished from the content of telephone conversations or e-mail communications.

[12] 15 U.S.C. § 1681 et seq.

[13] Intelligence Authorization Act for Fiscal Year 1996, Pub. L. No. 104-93, § 601(a), 109 Stat. 961, codified at 15 U.S.C. § 1681u (Supp. V. 1999).

[14] 15 U.S.C. § 1681u(a)-(b) (2000 & Supp. IV 2005).

[15] Patriot Act, § 358(g) (2001).

[16] Patriot Act, § 358(g) (2001).

4. The National Security Act

In the wake of the espionage investigation of former Central Intelligence Agency employee Aldrich Ames, Congress enacted an additional NSL authority in 1994 by amending the National Security Act of 1947. The National Security Act NSL statute authorizes the FBI to issue NSLs in connection with investigations of improper disclosure of classified information by government employees.[17] The statute permits the FBI to make requests to financial agencies and other financial institutions and consumer reporting agencies "in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination."[18]

National Security Act NSLs are rarely used by the FBI.

B. The FBI's Collection and Retention of Information Obtained From National Security Letters

To obtain approval for national security letters, FBI case agents must prepare: (1) an electronic communication (EC) seeking approval to issue the letter (approval EC), and (2) the national security letter itself. The approval EC explains the justification for opening or maintaining the investigation and why the information requested by the NSL is relevant to that investigation.

For field division-initiated NSLs, the Supervisory Special Agent of the case agent's squad, the Chief Division Counsel (CDC), and the Assistant Special Agent in Charge are responsible for reviewing the approval EC and the NSL prior to approval by the Special Agent in Charge. Division Counsel are required to review the NSLs to ensure their legal sufficiency – specifically, the relevance of the information requested to an authorized national security investigation.

The final step in the approval process occurs when the Special Agent in Charge or authorized FBI Headquarters official (the certifying official) certifies that the requested records are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and, with respect to investigations of "U.S. persons," that the investigation is not conducted solely on the basis of activities protected by the First Amendment. After making the required certifications, the official initials the approval EC and signs the national security letter.

During the time period covered by this review, the FBI had no policy or directive requiring the retention of signed copies of national security

---

[17] See H.R. Rep. No. 103-541 (1994) and H.R. Conf. Rep. No. 103-753 (1994), reprinted in 1994 U.S.C.C.A.N. 2703.

[18] 50 U.S.C. § 436(a)(1) (2000).

letters or any requirement to upload national security letters into the FBI's case management system, the Automated Case Support (ACS) system. We also found that the FBI has no uniform system for tracking responses to national security letters, either manually or electronically. Instead, individual case agents are responsible for following up with NSL recipients to ensure timely and complete responses, ensuring that the documents or electronic media provided to the FBI match the requests, analyzing the responses, and providing the documents or other materials to FBI intelligence or financial analysts who also analyze the information.

In some field offices, case agents are required to formally document their receipt of information from NSLs, including the date the information was received; the NSL subject's name, address, and Social Security number; and a summary of the information obtained. This document then is electronically uploaded into ACS. Once the data is available electronically, other case agents throughout the FBI can query ACS to identify information that may pertain to their investigations.

The FBI also evaluates the relationship between NSL-derived information and data derived from other investigative tools that are available in various databases. For example, when communication providers furnish telephone toll billing records and subscriber information on an investigative subject in response to an NSL, the data is uploaded into Telephone Applications, a specialized FBI database that can be used to analyze the calling patterns of a subject's telephone number. The FBI also places NSL-derived information into its Investigative Data Warehouse (IDW), a database that enables users to access, among other data, biographical information, photographs, financial data, and physical location information for thousands of known and suspected terrorists. IDW can be accessed by nearly 12,000 users, including FBI agents and analysts and members of Joint Terrorism Task Forces. Information derived from responses to national security letters that is uploaded into ACS and into Telephone Applications is periodically uploaded to IDW.

II. National Security Letters Issued by the FBI From 2003 Through 2005

In this section of the Executive Summary, we first discuss several problems with the FBI's Office of General Counsel National Security Letter database (OGC database) that affect the accuracy of the information in this database. We then present data on the FBI's use of national security letters from 2003 through 2005 based on data derived from the OGC database, the Department's semiannual classified reports to Congress on NSL usage, and our field work.

A. Inaccuracies in the FBI's National Security Letter Tracking Database

During the period covered by our review, the Department was required to file semiannual classified reports to Congress describing the total number of NSL requests issued pursuant to three of the five NSL authorities.[19] In these reports, the Department provided the number of requests for records and the number of investigations of different persons or organizations that generated NSL requests. These numbers were each broken down into separate categories for investigations of "U.S. persons or organizations" and "non-U.S. persons or organizations."

Total Number of NSL Requests. According to FBI data, the FBI issued approximately 8,500 NSL requests in CY 2000, the year prior to passage of the Patriot Act. After the Patriot Act, according to FBI data, the number of NSL requests increased to approximately 39,000 in 2003, approximately 56,000 in 2004, and approximately 47,000 in 2005.

However, we determined that these numbers were inaccurate because of three flaws in the manner in which the FBI records, forwards, and accounts for information about its use of NSLs.

First, we found incomplete or inaccurate information in the OGC database on the number of NSLs issued.[20] We compared the number of NSLs contained in the 77 case files we reviewed during our field work to those recorded in the OGC database and found approximately 17 percent more NSLs in the case files we examined than were recorded in the OGC database.

We also identified the total number of "requests" contained in the NSLs (such as requests in a single NSL for multiple telephone numbers or bank accounts) and compared that to the number of NSL requests recorded in the OGC database for those same national security letters. Overall, we found 22 percent more NSL requests in the case files we examined than were recorded in the OGC database.

---

[19] The Department was required to include in its semiannual classified reports only the number of NSL requests issued pursuant to the RFPA (financial records), the ECPA (telephone toll billing records, electronic communication transactional records and subscriber information (telephone or e-mail)), and the original FCRA NSL statute (consumer and financial institution identifying information), FCRAu. The Department was not required to report the number of NSL requests issued pursuant to the Patriot Act amendment to the FCRA (consumer full credit reports) or the National Security Act NSL statute (financial records, other financial information, and consumer reports). The requirement for public reports on certain NSL usage did not take effect until March 2006, which is after the period covered by this review.

[20] FBI-OGC utilizes a manual workflow process to enter required information into ACS. The information is transcribed into a Microsoft Access database which, during the period covered by our review, had limited analytical capabilities.

Second, we found that the FBI did not consistently enter the NSL approval ECs into ACS in a timely manner. As a result, this information was not in the OGC database when data was extracted for the semiannual classified reports to Congress, and the reports were therefore inaccurate. Although this data subsequently was entered in the OGC database, it was not included in later congressional reports because each report only includes data on NSL requests made in a specific 6-month period.

We determined that from 2003 through 2005 almost 4,600 NSL requests were not reported to Congress as a result of these delays in entering this information into the OGC database. In March 2006, the FBI acknowledged to the Attorney General and Congress that NSL data in the semiannual classified reports may not have been accurate and stated that the data entry delays affected an unspecified number of NSL requests.[21] After the FBI became aware of these delays, it took steps to reduce the impact of the delays to negligible levels for the second half of CY 2005.

Third, when we examined the OGC database, we found incorrect data entries. We discovered a total of 212 incorrect data entries, including blank data fields, typographical errors, and a programming feature that provides a default value of "0" for the number of "NSL requests." Taken together, these factors caused 477 NSL requests to be erroneously excluded from the Department's semiannual classified reports to Congress.

As a result of the delays in uploading NSL data and the flaws in the OGC database, the total numbers of NSL requests that were reported to Congress semiannually in CYs 2003, 2004, and 2005 were significantly understated. We were unable to fully determine the extent of the inaccuracies because an unknown amount of data relevant to the period covered by our review was lost from the OGC database when it malfunctioned. However, by comparing the data reflected in these reports to data in the OGC database for 2003 through 2005, we estimated that approximately 8,850 NSL requests, or 6 percent of NSL requests issued by the FBI during this period, were missing from the database.

Total Number of Investigations of Different U.S. Persons and Non-U.S. Persons. We found other inaccuracies in the OGC database that affect the accuracy of the total number of "investigations of different U.S. persons" or "investigations of different non-U.S. persons" that the Department reported to Congress. These included inaccuracies in the NSL approval ECs from which personnel in FBI-OGC's National Security Law Branch (NSLB) extract U.S. person/non-U.S. person data, as well as incorrect data entries in the OGC database.

---

[21] See Memorandum for the Attorney General, *Semiannual Report for Requests for Financial Records Made Pursuant to Title 12, United States Code (U.S.C.) Section 3414, Paragraph (a)(5), National Security Investigations/Foreign Collection* (March 23, 2006), at 2.

Incomplete or inaccurate entries resulted from several factors, including the inability of the OGC database to filter NSL requests for the same person in the same investigation (for example, "John T. Doe" and "J.T. Doe"); failure to account for NSL requests from different FBI divisions seeking information on the same person; and a default setting of "non-U.S. person" for the investigative subject for NSL requests seeking financial records and telephone toll billing/electronic communication transactional records. These errors resulted in the misidentification and understatement of the number of investigations of different U.S. persons that used NSLs.

The problems with the OGC database, including the loss of data because of a computer malfunction, also prevented us from determining with complete accuracy the number of investigations of different U.S. persons and different non-U.S. persons during which the FBI issued NSLs seeking financial records and for telephone toll billing/electronic communication transactional records.

Although we found that the data in the OGC database is not fully accurate or complete and, overall, significantly understates the number of FBI NSL requests, it is the only database that compiles information on the FBI's use of NSLs. Moreover, the data indicates the general levels and trends in the FBI's use of this investigative tool. We therefore relied in part on information compiled in the OGC database to respond to questions Congress directed us to answer regarding the FBI's use of NSLs.

B. National Security Letter Requests From 2003 Through 2005

1. The Total Number of NSL Requests

From 2003 through 2005, the FBI issued a total of 143,074 NSL requests. These included all requests issued for telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the ECPA NSL statute; records from financial institutions such as banks, credit card companies, and finance companies under the RFPA authority; requests seeking either financial institution or consumer identifying information (FCRAu) or consumer full credit reports (FCRAv); and requests pursuant to the National Security Act NSL authority.[22] The overwhelming majority of the NSL requests sought telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the ECPA NSL statute.

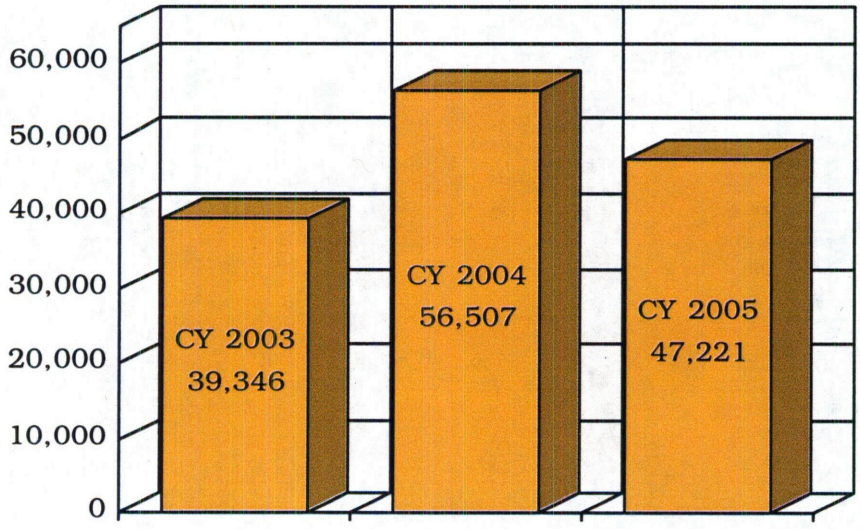
---

[22] As shown in Chart 4.1, the number of ECPA NSL requests increased in CY 2004, and then decreased in CY 2005. We determined that the spike in ECPA NSL requests in CY 2004 occurred because of the issuance of 9 ECPA NSLs in one investigation that contained requests for subscriber information on a total of 11,100 separate telephone numbers. If those nine NSLs are excluded from CY 2004, the number of NSL requests would show a moderate, but steady increase over the three years.

Chart 4.1 illustrates the total number of NSL requests issued in calendar years 2003 through 2005.

CHART 4.1

NSL Requests (2003 through 2005)



Sources: DOJ semiannual classified NSL reports to Congress and FBI-OGC NSL database as of May 2006

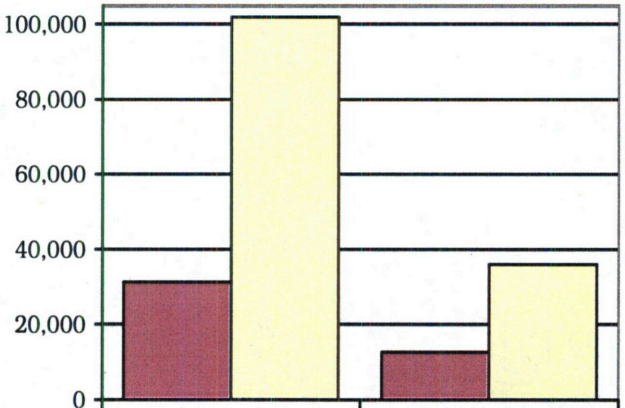
The number of NSL requests we identified significantly exceeds the number reported in the Department's first public annual report on NSL usage, issued in April 2006, because the Department was not required to include all NSL requests in that report. The Department's public report stated that in CY 2005 the FBI issued 9,254 NSL requests for information relating to U.S. persons, of which there were 3,501 NSLs relating to different U.S. persons. However, this does not include NSL requests under the ECPA NSL authority for telephone and e-mail subscriber information and NSL requests related to "non-U.S. persons," which were reported to Congress in the semiannual classified reports to Congress, or NSL requests not required to be reported to Congress under FCRAv for consumer full credit reports.

It is also important to note the total number of national security letter *requests* is different from the number of national security *letters*, because one "letter" may include more than one request. That is, during an investigation several national security letters may be issued, and each letter may contain several requests. For example, one letter to a telephone company may request information on seven telephone numbers. As a result, the numbers normally presented in the FBI's classified reports to Congress and in its public report are the number of requests made, not the number of letters issued. In this report, we follow that same approach. However, Chart 1.1 shows the relationship we found between the number of

NSLs and NSL requests from 2003 through 2005 in counterterrorism and counterintelligence cases.[23]

CHART 1.1

Relationship Between NSLs and NSL Requests (2003 through 2005)



	Counterterrorism	Counterintelligence
NSLs	31,246	12,754
NSL Requests	101,885	35,948

Source: FBI-OGC Database

2. Types of NSL Requests

As illustrated on Chart 4.2 below, during the 3 years of our review the balance of NSL requests related to investigations of U.S. persons versus non-U.S. persons shifted. The percentage of NSL requests generated from investigations of U.S. persons increased from about 39 percent of all NSL requests in CY 2003 to about 53 percent of all NSL requests in CY 2005.[24]

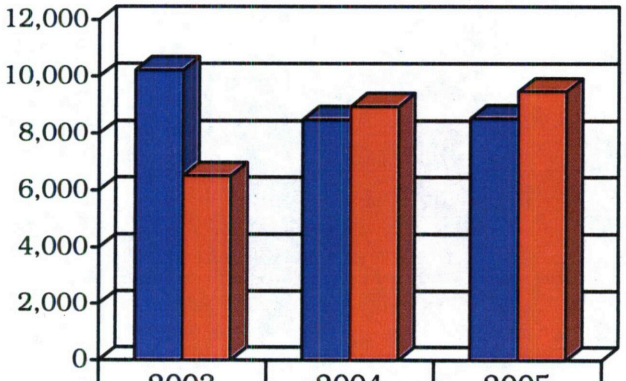
---

[23] The total number of requests in Chart 1.1 is not the same as in chart 4.1 because Chart 1.1 excludes NSL requests in cyber investigations and NSL requests that are not required to be reported to Congress.

[24] Chart 4.2 does not contain the same totals as Chart 4.1 because not all NSL requests reported to Congress identified whether they related to an investigation of a U.S. person or a non-U.S. person. Of the total number of NSL requests reported in the Department's semiannual classified reports to Congress for CY 2003 through CY 2005 (which included the ECPA, RFPA and FCRAu requests), 52,199 NSL requests identified whether the request for information related to a U.S. person or a non-U.S. person. The remaining NSL requests were for the ECPA NSLs seeking subscriber information for telephone numbers and Internet e-mail accounts and did not identify the subject's status as a U.S. person or non-U.S. person.

CHART 4.2

NSL Requests Reported to Congress Relating to U.S. Persons and non-U.S. Persons (2003 through 2005)



	2003	2004	2005
Non-U.S. Person	10,232	8,494	8,536
U.S. Person	6,519	8,943	9,475

Source: DOJ semiannual classified NSL reports to Congress

Our analysis of the FBI's use of NSL authorities during the 3 years also revealed that:

- Approximately 73 percent of the total number of NSL requests issued from 2003 through 2005 were issued in counterterrorism investigations, approximately 26 percent were issued in counterintelligence investigations, and less than 1 percent were issued in foreign computer intrusion cyber investigations;
- Of the 293 NSLs we examined in four field offices, 43.7 percent of the NSLs were issued during preliminary investigations and 56.3 percent were issued during full investigations.

III. The Effectiveness of National Security Letters as an Investigative Tool

The Patriot Reauthorization Act also directed the OIG to review the use and effectiveness of national security letters, including the importance of the information acquired and the manner in which information from national security letters is analyzed and disseminated within the Department, to other members of the intelligence community, and to other entities.

A. The Importance of the Information Acquired From National Security Letters to the Department's Intelligence Activities

FBI Headquarters and field personnel told us that they found national security letters to be effective in both counterterrorism and counterintelligence investigations. Many FBI personnel used terms to describe NSLs such as "indispensable" or "our bread and butter."

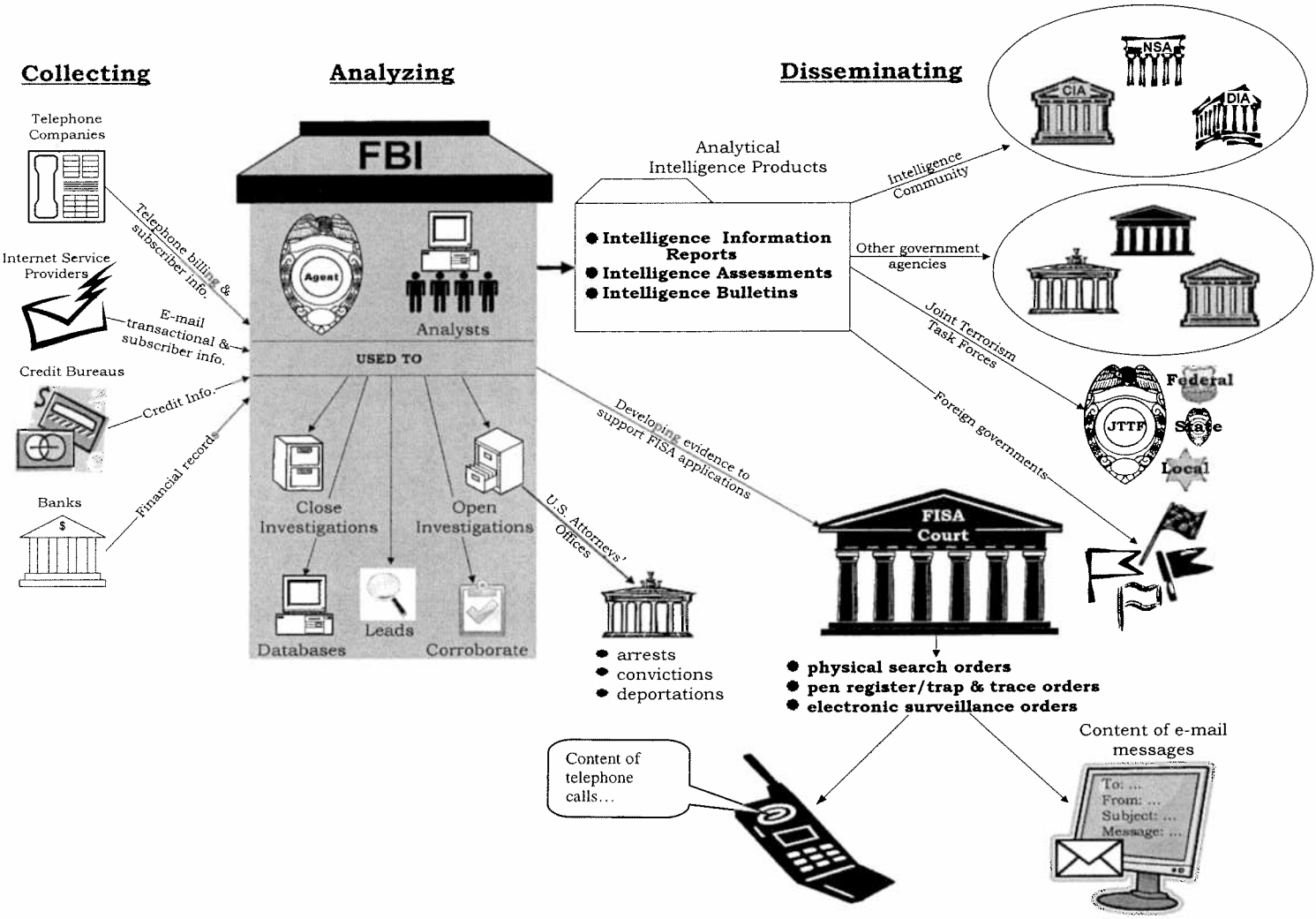
FBI personnel reported that the principal objectives for using NSLs are to:

- establish evidence to support Foreign Intelligence Surveillance Act (FISA) applications to the Foreign Intelligence Surveillance Court for electronic surveillance, physical searches, or pen register/trap and trace orders;
- assess communication or financial links between investigative subjects and others;
- collect information sufficient to fully develop national security investigations;
- generate leads for other field divisions, members of Joint Terrorism Task Forces, other federal agencies, or to pass to foreign governments;
- develop analytical products for distribution within the FBI, other Department components, other federal agencies, and the intelligence community;
- develop information that is provided to law enforcement authorities for use in criminal proceedings;
- collect information sufficient to eliminate concerns about investigative subjects and thereby close national security investigations; and
- corroborate information derived from other investigative techniques.

Diagram 5.1 illustrates the key uses of national security letters.

DIAGRAM 5.1

How the FBI Uses National Security Letters



1. Telephone toll billing records and subscriber information, and electronic communication transactional records

FBI agents and officials told us that telephone toll billing records and subscriber information and electronic communication transactional records obtained pursuant to ECPA NSLs enable FBI case agents to connect investigative subjects with particular telephone numbers or e-mail addresses and connect terrorism subjects and terrorism groups with each other. Analysis of subscriber information for telephone numbers and e-mail addresses also can assist in the identification of the investigative subject's family members, associates, living arrangements, and contacts. If the subject's associates are identified, case agents can generate new leads for their squad or another FBI field division, the results of which may complement the information obtained from the original NSL.

The FBI also informed us that the most important use of ECPA national security letters is to support FISA applications for electronic surveillance, physical searches, or pen register/trap and trace orders. FISA court orders for electronic surveillance may authorize the FBI to collect the content of telephone calls and Internet e-mail messages, information the FBI cannot obtain using NSLs.

2. Financial records

In addition, the FBI noted that NSLs are important tools for obtaining financial records related to suspected terrorists and terrorist organizations. The FBI's ability to track the movement of funds through financial institutions is essential to identify and locate individuals who provide financial support to terrorist operations. For example, transactional data obtained from banks and other financial institutions in response to RFPA national security letters can reveal the manner in which suspected terrorists conduct their operations, whether they are obtaining money from suspicious sources, and identify their spending patterns. Analysis of this data also can reveal the identity of the financial institutions used by the subject; the financial position of the subject; the existence of overseas wire transfers by or to the subject ("pass through" activity); loan transactions; evidence of money laundering; the subject's involvement in unconventional monetary transactions, including accounts that have more money in them than can be explained by ordinary income or the subject's employment; the subject's financial network; and payments to and from specific individuals.

In addition, NSLs issued pursuant to FCRA allow the FBI to obtain information from financial institutions from which an individual has sought or obtained credit and consumer identifying information limited to the subject's name, address and former addresses, places of employment, and former places of employment. The Patriot Act amendment to the FCRA authorizes the FBI to obtain consumer full credit reports, including records

of individual accounts, credit card transactions, and bank account activity. Information secured from both types of FCRA NSLs provide information that often is not available from other types of financial records. For example, consumer credit records provide confirming information about a subject (including name, aliases, and Social Security number); the subject's employment or other sources of income; and the subject's possible involvement in illegal activity, such as bank fraud or credit card fraud.

B. Analysis of Information Obtained From National Security Letters

The FBI performs various analyses and develops different types of analytical intelligence products using information obtained from national security letters. In counterterrorism investigations, once the case agent confirms that the response to the NSL matches the request, the most important function of the initial analysis is to determine if the records link the investigative subjects or other individuals whose records are sought to suspected terrorists or terrorist groups. In counterintelligence investigations, the case agent's initial analysis focuses on the subject's network and, in technology export cases, the subject's access to prohibited technologies.

Following the case agent's initial analysis, agents and analysts assigned to the FBI's Field Intelligence Groups (FIGs) and analysts with special expertise in the Headquarters Counterterrorism, Counterintelligence, and Cyber Divisions generate detailed analyses of intelligence information, some of which is derived from NSLs. One of the principal analytical intelligence products generated by FIG analysts are "link analyses" that typically illustrate the telephone numbers, Internet e-mail addresses, businesses, credit card transactions, addresses, places of employment, banks, and other data derived from the NSLs, other investigative tools, and open sources.

Information derived from NSLs also may be used in the development of a variety of written products that are shared with FBI personnel, distributed more broadly within the Department, shared with Joint Terrorism Task Forces, or disseminated to other members of the intelligence community. Among the intelligence products that use information obtained from NSLs are Intelligence Information Reports, which contain raw intelligence obtained from NSLs such as telephone numbers and Internet e-mail accounts; Intelligence Assessments, which are finished intelligence products that provide information on emerging developments and trends; and Intelligence Bulletins, which are finished intelligence products that contain general information on a topic rather than case-specific intelligence.

C. The FBI's Dissemination of Information Obtained From National Security Letters to Other Entities

Attorney General Guidelines and various information-sharing agreements require the FBI to share information with other federal agencies and the intelligence community. In addition, four of the five national security letter authorities expressly permit dissemination of information derived from NSLs to other federal agencies if the information is relevant to the authorized responsibility of those agencies and is disseminated pursuant to applicable Attorney General Guidelines.[25]

Pursuant to these statutes and directives, the FBI disseminated information derived from national security letters to other members of the intelligence community and to a variety of federal, state, and local law enforcement agencies during the period covered by our review. However, we could not determine the number of analytical intelligence products containing NSL-derived data that were disseminated from 2003 through 2005 because these products do not reference NSLs as the source of the information. Although none of the FBI or other Department officials we interviewed could estimate how often NSL-derived information was disseminated to other entities, they noted that when analytical intelligence products provided analyses of telephone or Internet communications or financial or consumer credit transactions, the products likely were derived in part from NSLs.

The principal entities outside the Department to whom information derived from NSLs are disseminated are members of the intelligence community and Joint Terrorism Task Forces (JTTFs). JTTFs across the country, composed of representatives of federal, state, and local law enforcement agencies, respond to, investigate, and share intelligence related to terrorist threats. Some designated task force members who obtain the necessary clearances to obtain access to FBI information, are authorized to access information stored in FBI databases such as ACS, Telephone Applications, and IDW which, as noted above, contain information derived from NSLs.

---

[25] See 12 U.S.C. § 3414(a)(5)(B)(Right to Financial Privacy Act); 18 U.S.C. § 2709(d)(Electronic Communications Privacy Act); 15 U.S.C.A. §1681u(f)(Fair Credit Reporting Act); and 50 U.S.C.A. § 436 (National Security Act). While the NSL statute permitting access to consumer full credit reports, 15 U.S.C. §1681v, does not explicitly authorize dissemination, it does not limit such dissemination.

D. Information From National Security Letters Provided to Law Enforcement Authorities for Use in Criminal Proceedings

1. Routine Information Sharing With United States Attorneys' Offices

Following the September 11 terrorist attacks, the Department established several initiatives that required the FBI to share information from its counterterrorism files with prosecutors in United States Attorneys' Offices (USAOs) in order to determine if criminal or other charges may be brought against individuals who are subjects of FBI counterterrorism investigations. As a result, information obtained from NSLs and analytical products derived from this information are routinely shared with terrorism prosecutors, although the source and details of the information may not be readily apparent to the prosecutors.

In addition, Anti-Terrorism Advisory Councils (ATACs), other terrorism prosecutors, and intelligence research specialists in the USAOs who review the FBI's investigative files may see the results of NSLs or the analyses of the information derived from NSLs in the investigative files or through access to the FBI's databases.

2. Providing Information to Law Enforcement Authorities for Use in Criminal Proceedings

Information from national security letters may also be used in criminal proceedings. As noted above, however, information derived from national security letters is not required to be marked or tagged as coming from NSLs when it is entered in FBI databases or when it is shared with law enforcement authorities outside the FBI.

As a result, FBI and DOJ officials told us they could not identify how often information derived from national security letters was provided to law enforcement authorities for use in criminal proceedings. To obtain a rough sense of how often the FBI provided NSL-derived information to federal law enforcement authorities for use in criminal proceedings, we asked FBI field personnel to identify (1) instances in which they referred targets of national security investigations to law enforcement authorities for prosecution and (2) whether in those instances they shared information derived from national security letters with law enforcement authorities.

The field offices that provided data on such referrals were unable to state in what percentage of these referrals they used NSLs. However, they provided examples of the use of NSLs in these proceedings, including instances in which NSLs were used in a counterintelligence case to obtain information on the subject's role in exporting sensitive U.S. military technology to a foreign country; and in a counterterrorism case in which NSLs generated subscriber information that supported FISA applications for

electronic surveillance on the subjects, leading to multiple convictions for conspiracy and providing material support to terrorists.

We learned from the responses that about half of the FBI's field divisions referred one or more counterterrorism investigation targets to law enforcement authorities for possible prosecution from 2003 through 2005. Of the 46 Headquarters and field divisions that responded to our request for information about referral of national security investigation targets, 19 divisions told us that they made no such referrals. Of the remaining 27 divisions, 22 divisions provided details about the type of information they referred and the nature of charges brought against these investigative subjects. In most cases, multiple charges were brought against the subjects, with the most common charges involving fraud (19), immigration (17), and money laundering (17).

IV. Improper or Illegal Use of National Security Letter Authorities

In this section of the Executive Summary, as directed by the Patriot Reauthorization Act, we report our findings on instances of "improper or illegal use" of national security letter authorities, including instances identified by the FBI as well as other instances identified by the OIG.[26]

A. Field Division Reports to FBI-OGC of 26 Possible IOB Violations Involving the Use of National Security Letters

The President's Intelligence Oversight Board (IOB) is directed by Executive Order 12863 to inform the President of any intelligence activities that "may be unlawful or contrary to Executive order or Presidential Directive." This directive has been interpreted by the Department and the IOB during the period covered by our review to include reports of violations of Department investigative guidelines or investigative procedures.[27]

We describe two groups of possible IOB violations related to NSLs that occurred during our review period (2003 through 2005). The first group

---

[26] In this report, we use the terms "improper or illegal use," as contained in the Patriot Reauthorization Act. As noted below, the improper or illegal uses of the national security letter authorities we found in our review did not involve criminal misconduct. However, as also noted below, the improper or illegal uses we found included serious misuses of national security letter authority.

[27] The FBI has developed an internal process for the self-reporting of possible IOB violations to FBI-OGC. During the period covered by our review, FBI-OGC issued 2 guidance memoranda describing the process by which FBI personnel were required to report such violations to FBI-OGC within 14 days of discovery. The reports were to include a description of the status of the subjects of the investigative activity, the legal authority for the investigation, the potential violation, and the date of the incident. FBI-OGC then reviewed the report, prepared a written opinion as to whether the matter should be sent to the IOB, and prepared the written communication to the IOB for those matters it decided to report.

consists of 26 possible IOB violations that were reported by FBI employees to FBI-OGC. The second group of incidents consists of 22 possible IOB violations which were not reported to FBI-OGC or the IOB that the OIG identified during our review of a sample of 77 investigative files in the 4 field divisions we visited.

1. Possible IOB Violations Identified by the FBI

We determined that from 2003 through 2005, FBI field divisions reported 26 possible IOB violations to FBI-OGC arising from the use of national security letter authorities. The 26 possible IOB violations included:

- Three matters in which the NSLs were signed by the appropriate officials but the underlying investigations were not approved or extended by the appropriate Headquarters or field supervisors.
- Four matters in which the NSLs did not satisfy the requirements of the pertinent NSL statute or the applicable Attorney General Guidelines. In three of these matters, the FBI obtained the information without issuing NSLs. One of these three matters involved acquisition of telephone toll billing records in the absence of investigative authority under the Attorney General's NSI Guidelines. In the fourth matter, the FBI sought and obtained consumer full credit reports in a counterintelligence investigation, which is not permitted by the Patriot Act amendment to the FCRA, 15 U.S.C. § 1681v.
- Nineteen matters in which the NSL recipient provided more information than was requested in the NSL or provided information on the wrong person, due either to FBI typographical errors or errors by recipients of the NSLs. Thirteen of these matters involved requests for telephone toll billing records, 4 involved requests for electronic communication transactional records, and 2 involved requests for telephone subscriber information.

In 15 of the 26 matters identified by the FBI as possible IOB violations, the subject was a "U.S. person," and in 8 of the matters the subject was a "non-U.S. person." In one of the matters, the subject was a presumed "non-U.S. person," in one there was no subject because there was no underlying investigation, and in another the status of the subject could not be determined.

In total, 22 of the 26 possible IOB violations were due to FBI errors, while 4 were due to third-party errors. The FBI errors included typographical errors on the telephone numbers or e-mail addresses listed in the NSLs; telephone numbers that did not belong to the targets of NSLs; receipt of responses to three telephone toll billing record requests when the investigative authority was not properly authorized or had lapsed; receipt of telephone toll billing records and subscriber information from a telephone

company employee on nine separate occasions without issuing ECPA national security letters; and a FCRA NSL request for a consumer full credit report in a counterintelligence case. The errors also included instances in which the FBI obtained information without issuing the required NSL, including receipt of telephone toll billing records in the absence of an open national security investigation through informal contact with FBI Headquarters Counterterrorism Division's Communications Analysis Unit without issuing an ECPA NSL and accessing financial records through the use of FISA authorities rather than by issuing an RFPA NSL.

The four third-party errors included the NSL recipient providing prohibited content information (including voice messages) in response to an ECPA NSL for telephone toll billing records; and a third party providing prohibited content information (including e-mail content and images) in response to three ECPA NSLs requesting electronic communication transactional records.

Twenty of the 26 possible IOB violations were timely reported within 14 days of discovery to FBI-OGC in accordance with FBI policy. However, 6 were not reported in a timely fashion, taking between 15 days and 7 months to report. FBI records show that FBI-OGC reported 19 of the 26 possible violations to the IOB and decided not to report the 7 remaining matters.

2. OIG Analysis Regarding Possible IOB Violations Identified by the FBI

Our examination of the 26 possible IOB violations reported to FBI-OGC did not reveal deliberate or intentional violations of NSL statutes, the Attorney General Guidelines, or internal FBI policy. Although the majority of the possible violations – 22 of 26 – arose from FBI errors, most of them occurred because of typographical errors or the case agent's good faith but erroneous belief that the information requested related to an investigative subject.

However, three of the possible IOB violations arising from FBI errors demonstrated FBI agents' unfamiliarity with the constraints on NSL authorities. In one instance, an FBI analyst was unaware of the statutory, Attorney General Guidelines, and internal FBI policy requirements that NSLs can only be issued during a national security investigation and must be signed by the Special Agent in Charge of the field division. In the two other matters, probationary agents erroneously believed that they were authorized to obtain records about investigative subjects – without issuing NSLs – from information derived from FISA electronic surveillance orders. In these instances, it is clear that the agents, and in one instance the squad supervisor, did not understand the interrelationship between FISA authorities and national security letter authorities.

With regard to the FBI's decisions whether to report the possible violations to the IOB, we concurred in FBI-OGC's analysis with one

exception. We disagreed with the FBI-OGC decision not to report the possible violation to the IOB related to the FBI's acquisition of telephone toll billing records and subscriber information relating to a "non-U.S. person" from a telephone company employee on nine occasions without issuing an NSL. FBI-OGC reasoned that because the investigative subject was a "non-U.S. person" agent of a foreign power, the only determination it had to reach was whether the FBI's failure to conform to its internal administrative requirements was reportable "as a matter of policy" to the IOB. In light of FBI-OGC's decisions to report at least four other IOB violations that were triggered by NSLs in which the investigative subject or the target of the NSL was a "non-U.S. person," we disagreed with FBI-OGC's determination that this matter should not be reported to the IOB.

B. Additional Possible IOB Violations Arising From National Security Letters Identified by the OIG During Our Field Visits

1. Possible IOB Violations Identified by the OIG

In addition to the 26 possible IOB violations identified by the FBI in this 3-year review period, we found 22 additional possible IOB violations during our review of 77 investigative files in the 4 field offices we visited.

In those 77 files, we reviewed 293 NSLs. We identified 22 NSL-related possible IOB violations that arose in the course of 17 separate investigations. None of these possible violations was reported to FBI-OGC or the IOB. Thus, we found that 22 percent of the investigative files we reviewed (17 of 77) contained one or more possible IOB violations that were not reported to FBI-OGC or the IOB.

The possible IOB violations we identified fell into three categories: improper authorization for the NSL (1), improper requests under the pertinent national security letter statutes (11), and unauthorized collections (10). The possible violations included:

- One NSL for telephone toll billing records was issued 22 days after the authorized period for the investigation had lapsed.
- Nine NSLs involved improper requests under the FCRA. Two of the 9 NSLs issued during one investigation requested consumer full credit reports during a counterintelligence investigation, while the statute authorizes this type of NSL only in international terrorism investigations. The approval ECs for 3 of these 9 NSLs listed FCRAv as the authority for the request but the NSLs included the certification of relevance language either for the RFPA or FCRAu NSL authorities. In addition, 4 of these 9 NSLs were FCRAv requests where the types of records approved by field supervisors differed from the records requested in the NSL.

- Two NSLs referenced the ECPA as authority for the request but sought content information not permitted by the statute. In one instance, the NSL requested information that arguably was content information and associated subscriber information.[28] The second NSL requested financial records associated with two e-mail addresses but requested the information under the ECPA rather than the RFPA, which only authorizes access to financial records.
- Ten NSLs involved the FBI's receipt of unauthorized information. In 4 instances, the FBI received telephone toll billing records or subscriber information for telephone numbers that were not listed in the national security letters. In these instances the provider either erroneously furnished additional records for another telephone number associated with the requested number or made transcription errors when querying its systems for the records. In 4 instances, the FBI received telephone toll billing records information and electronic communication transactional records for longer periods than that specified in the NSL – periods ranging from 30 days to 81 days. One NSL sought subscriber records pursuant to the ECPA, but the recipient provided the FBI with toll billing records. One NSL sought financial institution and consumer identifying information about an individual pursuant to FCRAu. However, the recipient erroneously gave the FBI the individual's consumer full credit report, which is available pursuant to another statute, FCRAv.

Twelve of the 22 possible IOB violations identified by the OIG were due to FBI errors, and 10 were due to errors on the part of third party recipients of the NSLs.[29]

---

[28] When we examined the records provided to the FBI in response to this NSL, however, we determined that the requested information was not furnished to the FBI.

[29] Our report also discusses another noteworthy possible IOB violation involving the issuance of an NSL seeking educational records from a North Carolina university. In that matter, which we learned of through press accounts, the FBI's Charlotte Division was in the process of seeking a grand jury subpoena for educational records about an investigative subject to determine whether the subject was involved in the July 2005 London subway and bus bombings. The NSL sought several categories of records, including applications for admission, housing information, emergency contacts, and campus health records. According to press accounts, university officials said that the FBI had tried to use an NSL to demand more information than the law permitted and declined to honor the national security letter. A grand jury subpoena was thereafter served on the university, and the university produced the records. In this instance, the FBI sought records it was not authorized to obtain pursuant to an ECPA national security letter.

2. OIG Analysis Regarding Possible IOB Violations Identified by the OIG

In the limited file review we conducted of 77 investigative files in 4 FBI field offices, we identified nearly as many NSL-related possible IOB violations (22) as the number of NSL-related possible violations that the FBI identified (26) in reports from all FBI Headquarters and field divisions for the same 3-year period. We found that 22 percent of the investigative files that we reviewed contained at least one possible IOB violation that was not reported to FBI-OGC or the IOB. Because we have no reason to believe that the number of NSL-related possible IOB violations we identified in the four field offices was skewed or disproportionate to the number of possible IOB violations that exist in other offices, our findings suggest that a significant number of NSL-related possible IOB violations throughout the FBI have not been identified or reported by FBI personnel.

Our review did not reveal intentional violations of national security letter authorities, the Attorney General Guidelines, or internal FBI policy. Rather, we found confusion about the authorities available under the various NSL statutes. Our interviews of FBI field personnel and review of e-mail exchanges between NSLB attorneys and Division Counsel indicated that field personnel sometimes confused the two different authorities under the FCRA: the original FCRA provision that authorized access to financial institution and consumer identifying information in both counterterrorism and counterintelligence cases (15 U.S.C. §§ 1681u(a) and (b)), and the Patriot Act provision that amended the FCRA to authorize access to consumer full credit reports in international terrorism investigations where "such information is necessary for the agency's conduct of such investigation, activity or analysis" (15 U.S.C. § 1681v). Although NSLB sent periodic guidance and "all CDC" e-mails to clarify the distinctions between the two NSLs, we found that the problems and confusion persisted.

In addition, we believe that many of the violations occurred because case agents and analysts do not consistently cross check the approval ECs with the text of proposed NSLs or verify upon receipt that the information supplied by the NSLs recipient matches the requests. We also question whether case agents or analysts reviewed the records provided by the NSL recipients to determine if records were received beyond the time period requested or, if they did so, determined that the amount of excess information received was negligible and did not need to be reported.

Our review also found that the FBI did not issue comprehensive guidance describing the types of NSL-related infractions that needed to be reported to FBI-OGC as possible IOB violations. We noted frequent exchanges between Division Counsel and NSLB attorneys about what should and should not be reported as possible IOB violations which we believe showed significant confusion about the reporting requirements. However, the FBI did not issue comprehensive guidance about NSL-related

infractions until November 2006, more than 5 years after the Patriot Act was enacted. We believe the lack of guidance contributed to the high rate of unreported possible IOB violations involving national security letters that we found.

As was the case with the NSL-related possible IOBs identified by the FBI, the possible violations identified or reviewed by the OIG varied in seriousness. Among the most serious matters resulting from FBI errors were the two NSLs requesting consumer full credit reports in a counterintelligence case and the NSL requesting educational records from a university, ostensibly pursuant to the ECPA. In these three instances, the FBI misused NSL authorities. Less serious infractions resulting from FBI errors were the seven matters in which three levels of supervisory review failed to detect and correct NSLs that contained incorrect certifications or sought records not referenced in the approval ECs. While the FBI was entitled to obtain the records sought or obtained in these seven NSLs, the lapses in oversight indicate that the FBI should reinforce the need for careful preparation and review of all documentation supporting the use of NSL authorities.

C. Improper Use of National Security Letter Authorities by FBI Headquarters Counterterrorism Division Units Identified by the OIG

We identified two ways in which FBI Headquarters Counterterrorism Division units circumvented the requirements of national security letter authorities or issued NSLs contrary to the Attorney General's NSI Guidelines and internal FBI policy. First, we learned that on over 700 occasions the FBI obtained telephone toll billing records or subscriber information from 3 telephone companies without first issuing NSLs or grand jury subpoenas. Instead, the FBI issued so-called "exigent letters" signed by FBI Headquarters Counterterrorism Division personnel who were not authorized to sign NSLs. The letters stated the records were requested due to "exigent circumstances" and that subpoenas requesting the information had been submitted to the U.S. Attorney's Office for processing and service "as expeditiously as possible." However, in most instances there was no documentation associating the requests with pending national security investigations. In addition, while some witnesses told us that many of the exigent letters were issued in connection with fast-paced investigations, many were not issued in exigent circumstances, and the FBI was unable to determine which letters were sent in emergency circumstances due to inadequate recordkeeping. Further, in many instances after obtaining such records from the telephone companies, the FBI issued NSLs after the fact to "cover" the information obtained, but these after-the-fact NSLs sometimes were issued many months later.

Second, we determined that FBI Headquarters personnel regularly issued national security letters seeking electronic communication transactional records exclusively from "control files" rather than from "investigative files," a practice not permitted under FBI policy. If NSLs are issued exclusively from control files, the NSL approval documentation does not indicate whether the NSLs are issued in the course of authorized investigations or whether the information sought in the NSLs is relevant to those investigations. Documentation of this information is necessary to establish compliance with NSL statutes, the Attorney General's NSI Guidelines, and internal FBI policy.

We describe below these practices, how they were discovered, and what actions the FBI took to address the issues.

1. Using "Exigent Letters" Rather Than ECPA National Security Letters

The FBI entered into contracts with three telephone companies between May 2003 and March 2004 to obtain telephone toll billing records or subscriber information more quickly than by issuing ECPA NSLs. The requests for approval to obligate funds for each of these contracts referred to the Counterterrorism Division's need to obtain telephone toll billing data from telephone companies as quickly as possible. The three memoranda stated that:

> Previous methods of issuing subpoenas or National Security Letters (NSL) and having to wait weeks for their service, often via hard copy reports that had to be retyped into FBI databases, is insufficient to meet the FBI's terrorism prevention mission.

The three memoranda also stated that the telephone companies would provide "near real-time servicing" of legal process, and that once legal process was served telephone records would be provided.

The Communications Analysis Unit (CAU) in the Counterterrorism Division's Communications Exploitation Section (CXS) worked directly with telephone company representatives in connection with these contracts. CAU personnel told FBI employees that it expected to receive national security letters or other legal process before it obtained records from the telephone companies.

Using as its model a letter used by the FBI's New York Division to request telephone records in connection with the FBI's criminal investigations of the hijackers involved in the September 11 attacks, CAU issued over 700 exigent letters to the three telephone companies between

March 2003 and December 2005 that requested telephone toll billing records or subscriber information.[30] The letters stated:

> Due to exigent circumstances, it is requested that records for the attached list of telephone numbers be provided. Subpoenas requesting this information have been submitted to the U.S. Attorney's Office who will process and serve them formally to [information redacted] as expeditiously as possible.

We determined that, contrary to the provisions of the contracts and the assertions in CAU's briefings that the FBI would obtain telephone records only after it served NSLs or grand jury subpoenas, the FBI obtained telephone toll billing records and subscriber information in response to the exigent letters prior to serving NSLs or grand jury subpoenas. Moreover, CAU officials told us that contrary to the assertion in the exigent letters, subpoenas requesting the information had not been provided to the U.S. Attorney's Office before the letters were sent to the telephone companies.

In total, between March 2003 and December 2005 the FBI issued at least 739 exigent letters to the three telephone companies requesting information on approximately 3,000 different telephone numbers. The exigent letters were signed by CXS Section Chiefs, CAU Unit Chiefs, and subordinate CAU personnel – including intelligence analysts – none of whom was delegated authority to sign NSLs.

CAU personnel told us that many of the exigent letters were generated in connection with significant Headquarters-based counterterrorism investigations as well as investigations in which the FBI provided assistance to foreign counterparts, such as investigations of the July 2005 London bombings, and that some CAU personnel believed some requests were urgent. However, when CAU personnel gave the exigent letters to the three telephone companies, they did not provide to their supervisors any documentation demonstrating that the requests related to pending FBI investigations. This documentation is necessary to establish compliance with the ECPA NSL statute, the NSI Guidelines, and internal FBI policy.

Moreover, when CAU requested telephone records from the three telephone companies pursuant to exigent letters, there sometimes were no open investigations tied to the request. In the absence of pending investigations, CAU sent leads either to the Headquarters Counterterrorism Division or to field offices that were geographically associated with the

---

[30] Following the September 11 attacks, the FBI's New York Division established a relationship with one of the major telephone companies to obtain quick responses to requests for telephone toll billing records or subscriber information in connection with its criminal investigations of the 19 hijackers. Although the New York Division generally obtained grand jury subpoenas to obtain this information, it frequently provided a "placeholder letter," sometimes referred to as an "exigent letter," to the telephone company if the grand jury subpoena was not yet available.

requests asking them to initiate new investigations from which the after-the-fact NSLs could be issued. However, Counterterrorism Division units and field personnel often resisted generating the documentation for these new investigations or declined to act on the leads, primarily for three reasons. First, CAU often did not provide the operating units with sufficient information to justify the initiation of an investigation. Second, on some occasions the documentation CAU supplied to the field divisions did not disclose that the FBI had already obtained the information from the telephone companies.[31] When the field offices learned that the records had already been received, they complained to attorneys in FBI-OGC's National Security Law Branch (NSLB) that this did not seem appropriate. Third, since Headquarters and field divisions were unfamiliar with the reasons underlying the requests, they believed that the CAU leads should receive lower priority than their ongoing investigations.

NSLB attorneys responsible for providing guidance on the FBI's use of national security letter authorities told us that they were not aware of CAU's practice of using exigent letters until late 2004. When an NSLB Assistant General Counsel learned of the practice at that time, she believed that the practice did not comply with the ECPA NSL statute. For nearly 2 years after learning of the practice, beginning in late 2004, NSLB attorneys counseled CAU officials to take a variety of actions, including: to discontinue use of exigent letters except in true emergencies; obtain more details to be able to justify associating the information with an existing national security investigation or to request the initiation of a new investigation; issue duly authorized NSLs promptly after the records were provided in response to the exigent letters; modify the letters to reference national security letters rather than grand jury subpoenas; and consider opening "umbrella" investigations out of which NSLs could be issued in the absence of another pending investigation. In addition, NSLB offered to dedicate personnel to expedite issuance of CAU NSL requests (as it had done for other high priority matters requiring expedited NSLs). However, CAU never pursued this latter option.

In addition, we found that the FBI did not maintain a log to track whether it issued NSLs or grand jury subpoenas after the fact to cover the records provided in response to the exigent letters, relying instead upon the three telephone companies to track whether NSLs or grand jury subpoenas were later issued. As a result, when we asked the FBI to match NSLs and grand jury subpoenas issued to the three telephone companies with a random sample of the exigent letters, the FBI was unable to provide reliable

---

[31] Similarly, when CAU on occasion asked the NSLB Deputy General Counsel to issue national security letters to cover information already obtained from the telephone companies in response to the exigent letters, CAU sometimes did not disclose in the approval documentation that the records already had been provided in response to the exigent letters. An NSLB Assistant General Counsel complained to CAU personnel about these omissions in December 2004.

requests asking them to initiate new investigations from which the after-the-fact NSLs could be issued. However, Counterterrorism Division units and field personnel often resisted generating the documentation for these new investigations or declined to act on the leads, primarily for three reasons. First, CAU often did not provide the operating units with sufficient information to justify the initiation of an investigation. Second, on some occasions the documentation CAU supplied to the field divisions did not disclose that the FBI had already obtained the information from the telephone companies.[31] When the field offices learned that the records had already been received, they complained to attorneys in FBI-OGC's National Security Law Branch (NSLB) that this did not seem appropriate. Third, since Headquarters and field divisions were unfamiliar with the reasons underlying the requests, they believed that the CAU leads should receive lower priority than their ongoing investigations.

NSLB attorneys responsible for providing guidance on the FBI's use of national security letter authorities told us that they were not aware of CAU's practice of using exigent letters until late 2004. When an NSLB Assistant General Counsel learned of the practice at that time, she believed that the practice did not comply with the ECPA NSL statute. For nearly 2 years after learning of the practice, beginning in late 2004, NSLB attorneys counseled CAU officials to take a variety of actions, including: to discontinue use of exigent letters except in true emergencies; obtain more details to be able to justify associating the information with an existing national security investigation or to request the initiation of a new investigation; issue duly authorized NSLs promptly after the records were provided in response to the exigent letters; modify the letters to reference national security letters rather than grand jury subpoenas; and consider opening "umbrella" investigations out of which NSLs could be issued in the absence of another pending investigation. In addition, NSLB offered to dedicate personnel to expedite issuance of CAU NSL requests (as it had done for other high priority matters requiring expedited NSLs). However, CAU never pursued this latter option.

In addition, we found that the FBI did not maintain a log to track whether it issued NSLs or grand jury subpoenas after the fact to cover the records provided in response to the exigent letters, relying instead upon the three telephone companies to track whether NSLs or grand jury subpoenas were later issued. As a result, when we asked the FBI to match NSLs and grand jury subpoenas issued to the three telephone companies with a random sample of the exigent letters, the FBI was unable to provide reliable

---

[31] Similarly, when CAU on occasion asked the NSLB Deputy General Counsel to issue national security letters to cover information already obtained from the telephone companies in response to the exigent letters, CAU sometimes did not disclose in the approval documentation that the records already had been provided in response to the exigent letters. An NSLB Assistant General Counsel complained to CAU personnel about these omissions in December 2004.

evidence to substantiate that NSLs or other legal process was issued to cover the FBI's receipt of records requested in the sample exigent letters.

We also were troubled that the FBI issued exigent letters that contained factual misstatements indicating that "[s]ubpoenas requesting this information have been submitted to the U.S. Attorney's Office who will process and serve them formally . . . as expeditiously as possible."[32] In fact, in examining the documents CAU provided in support of the first 25 of the 88 randomly selected exigent letters, we could not confirm one instance in which a subpoena had been submitted to any United States Attorney's Office before the exigent letter was sent to the telephone companies.

We concluded that, as a consequence of the CAU's use of the exigent letters to acquire telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs or grand jury subpoenas, the FBI circumvented the requirements of the ECPA NSL statute and violated the NSI Guidelines and internal FBI policies. These actions were compounded by the fact that CAU used exigent letters in non-emergency circumstances, failed to ensure that there were duly authorized investigations to which the requests could be tied, and failed to ensure that NSLs were issued promptly after the fact pursuant to existing or new counterterrorism investigations.

In evaluating these matters, it is also important to recognize the significant challenges the FBI was facing during the period covered by our review. After the September 11 terrorist attacks, the FBI implemented major organizational changes to seek to prevent additional terrorist attacks in the United States, such as overhauling its counterterrorism operations, expanding its intelligence capabilities, beginning to upgrade its information technology systems, and seeking to improve coordination with state and local law enforcement agencies. These changes occurred while the FBI and its Counterterrorism Division has had to respond to continuing terrorist threats and conduct many counterterrorism investigations, both internationally and domestically. In addition, the FBI developed specialized operational support units that were under significant pressure to respond quickly to potential terrorist threats. It was in this context that the FBI used exigent letters to acquire telephone toll billing records and subscriber information on approximately 3,000 different telephone numbers without first issuing ECPA national security letters. We also recognize that the FBI's use of so-called "exigent letters" to obtain the records without first issuing NSLs was undertaken without the benefit of advance legal consultation with FBI-OGC.

---

[32] The FBI's reference to grand jury subpoenas in the exigent letters rather than to national security letters appears to be the result of CAU's use of the New York Division's model letter for exigent letters sent to a telephone company in connection with the New York Division's criminal investigations of the September 11 hijackers.

However, we believe none of these circumstances excuses the FBI's circumvention of the requirements of the ECPA NSL statute and its violations of the Attorney General's NSI Guidelines and internal FBI policy governing the use of national security letters.

2. National Security Letters Issued From Headquarters Control Files Rather Than From Investigative Files

The national security letter statutes and the Attorney General's NSI Guidelines authorize the issuance of national security letters only if the information sought is relevant to an "authorized investigation." Within the FBI, the only types of investigations in which NSLs may be used are national security investigations.

For purposes of conducting its investigations and compiling information obtained from the use of various investigative authorities, agents may seek supervisory approval to establish an "investigative file." The FBI also provides for the establishment of non-investigative files, referred to as "control files" or "repository files," which are used to store information (such as the results of indices searches of the names of individuals who are relevant to FBI investigations) that may never rise to the level of predication necessary to initiate a national security investigation. The FBI's National Foreign Intelligence Program (NFIP) Manual states that control files are not investigative files and are not considered preliminary investigations or full investigations.

Unless national security letters are issued from investigative files, case agents and their supervisors – and internal and external reviewers – cannot determine whether the requests are tied to substantive investigations that have established the required evidentiary predicate for issuing NSLs. As the FBI General Counsel told us, the only way to determine if the information requested in a national security letter is relevant to an authorized investigation is to have an investigative file to which the NSL request can be tied or to have the connection described in the NSL approval EC.

Notwithstanding these policies, we found that in two circumstances the FBI relied exclusively on "control files" rather than "investigative files" to initiate approval for the issuance of many national security letters, in violation of FBI policy. In the first circumstance, from 2003 through 2005, CAU initiated NSL approval memoranda for approximately 300 national security letters in connection with a classified special project from a Headquarters control file. All of the resulting NSLs sought telephone toll billing records, subscriber information, or electronic communication transactional records pursuant to the ECPA NSL statute, but none of the approval ECs referred to the case number of any specific pending FBI investigation.

Since CAU officials are not authorized to sign NSLs, CAU sent leads to field offices to initiate the process to issue NSLs, but CAU met resistance from some field personnel who questioned the adequacy of predication to initiate a national security investigation.[33] To address the problem, the Counterterrorism Division opened a special project control file from which the CAU sought approval from NSLB to issue NSLs for subscriber information.

In December 2006, after considering a number of options that would comply with the ECPA NSL statute, the Attorney General's NSI Guidelines, and internal FBI policy, the FBI initiated an "umbrella" investigative file from which national security letters related to this classified project could be issued.

In the second circumstance, the FBI issued at least six national security letters from 2003 through 2005 solely on the authority of a control files established by the Counterterrorism Division's Electronic Surveillance Operations and Sharing Unit (EOPS) in the Communications Exploitation Section and another control file.[34] The six NSLs sought information from Internet service providers. None of the approval ECs accompanying the requests for these NSLs referred to the case number of any specific pending FBI investigation. Following questions raised by the OIG in this review, the NSLB Deputy General Counsel told us that she has advised the EOPS Unit Chief to discontinue requesting approval of national security letters issued exclusively out of control files.

D. Failure to Adhere to FBI Internal Control Policies on the Use of National Security Letter Authorities

During our field visits, we also examined FBI investigative files to determine whether the field office's use of national security letters violated FBI internal control policies. In our review of the 77 investigative files and 293 national security letters in 4 FBI field offices, we identified repeated failures to adhere to FBI-OGC guidance regarding the documentation necessary for approval of national security letters. Forty-six of the 77 files we examined (60 percent) contained one or more of the following infractions: (1) NSL approval memoranda that were not reviewed and initialed by one or more of the required field supervisors or Division Counsel; (2) NSL approval memoranda that did not contain the required information; and (3) NSLs that did not contain the certifications or other information required by the authorizing statutes.

---

[33] The classified nature of the project was such that few FBI Headquarters officials or FBI-OGC attorneys were authorized to know the predication for the requests.

[34] Problems with the FBI's NSL database make it impossible to determine the precise number of national security letters the FBI issued in this second category.

Approximately 7 percent of the approval memoranda we examined (22 of 293) did not reflect review or approval by one or more of the field supervisors who are required to approve NSL requests. They included failures to document approval by the Special Agents in Charge (4); Assistant Special Agents in Charge (18); Supervisory Special Agents (8); or the Chief Division Counsel or Assistant Division Counsel (3).

Thirty-four percent of the approval memoranda we examined (99 of 293) did not contain one or more of the four elements required by FBI internal policy. Approval memoranda failed to reference the statute authorizing the FBI to obtain the information or cited the wrong statute (16); failed to reference the "U.S. person" or "non-U.S. person" status of the investigative subject (66); failed to specify the type and number of records requested (34); and failed to recite the required predication for the request (7).

Approximately 2 percent of the national security letters we examined (5 of 293) did not include at least one of the required elements, including failures to reference an NSL statute or referencing the wrong statute. In addition, we were unable to comprehensively audit the field divisions' compliance with the requirement that Special Agents in Charge sign national security letters because three of the four divisions we visited did not maintain signed copies of their national security letters. The Special Agent in Charge of the fourth division maintained a control file with copies of all NSLs he signs, but this practice was instituted only during the last year of our review period.

V. Other Noteworthy Fact and Circumstances Related to the FBI's Use of National Security Letters

As directed by the Patriot Reauthorization Act, our report includes "other noteworthy facts and circumstances" related to the FBI's use of national security letters that we found during our review.

A. Using the "Least Intrusive Collection Techniques Feasible"

The NSI Guidelines that were in effect during most of the period covered by our review state:

> Choice of Methods. 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. 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.[35]

However, during our review we found that no clear guidance was given to FBI agents on how to reconcile the limitations expressed in the Attorney General Guidelines, which reflect concerns about the impact on privacy of FBI collection techniques, with the expansive authorities in the NSL statutes.

These issues raise difficult questions that regularly arise regarding the FBI's use of national security letters, such as (1) whether case agents should access NSL information about parties two or three steps removed from their subjects without determining if these contacts reveal suspicious connections; (2) whether there is an evidentiary threshold beyond "relevance to an authorized investigation" that should be considered before financial records or full credit histories are obtained on persons who are not investigative subjects; and (3) whether NSLs are more or less intrusive than other investigative techniques authorized for use during national security investigations, such as physical surveillance. On the other hand, if agents are hindered from using all types of NSLs at early stages of national security investigations, this may compromise the FBI's ability to pursue critical investigations of terrorism or espionage threats or to reach resolution expeditiously that certain subjects do not pose threats.

The impact of the FBI's investigative choices when using national security letters is magnified by three factors. First, the FBI generates tens of thousands of NSLs per year on the authority of Special Agents in Charge, and the predication standard – relevance to an authorized investigation – can easily be satisfied. Second, we found that FBI Division Counsel in field offices have asked NSLB attorneys in FBI Headquarters for ad hoc guidance on application of the "least intrusive collection techniques feasible" proviso, suggesting a need for greater clarity. Third, neither the Attorney General's NSI Guidelines nor internal FBI policies require the purging of information derived from NSLs in FBI databases, regardless of the outcome of the investigation. Thus, once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases.

We recognize that there cannot be one model regarding the use of NSLs in all types of national security investigations, and that the FBI cannot issue definitive guidance addressing when and what types of NSLs should issue at each stage of investigations. The judgment of FBI agents and their supervisors, coupled with review by Chief Division Counsel and Special Agents in Charge or senior Headquarters officials, are critical to ensuring

---

[35] NSI Guidelines, § I(B)(2).

the appropriate use of NSLs and preventing overreaching. However, we believe that the meaning and application of the Attorney General Guidelines' proviso calling for use of the "least intrusive collection techniques feasible" to the FBI's use of national security letter authorities should be addressed in general guidance as well as in the training of special agents, Chief Division Counsel, and all FBI officials authorized to sign NSLs. With the FBI's increasing reliance on national security letters as an investigative technique, such guidance and training would be helpful in assisting FBI personnel in reconciling the important privacy considerations that underlie the Attorney General Guidelines' proviso with the FBI's mission to detect and deter terrorist attacks and espionage threats.

B. Telephone "Toll Billing Records Information"

We found that FBI agents and attorneys frequently have questions regarding the types of records they can obtain when requesting "toll billing records information," a term that is not defined in the ECPA NSL statute. In the absence of a statutory definition or case law interpreting this phrase, different electronic communication service providers produce different types of information in response to the FBI's ECPA national security letter requests for these records. We found that ongoing uncertainty about the meaning of the phrase "toll billing records information" has generated multiple inquiries by Division Counsel to NSLB attorneys and confusion on the part of various communication providers. In light of this recurring issue, we recommend that the Department consider seeking a legislative amendment to the ECPA to define the phrase "toll billing records information."

C. The Role of FBI Division Counsel in Reviewing National Security Letters

FBI Division Counsel are responsible for identifying and correcting erroneous information in NSLs and NSL approval memoranda, resolving questions about the scope of the NSL statutes, ensuring adequate predication for NSL requests, and providing advice on issues concerning the collection of unauthorized information through national security letters. However, Division Counsel are not in the chain of review or approval for the initiation of national security investigations. Thus, by the time Division Counsel see the first NSL request in an investigation, the investigation has already been approved by a field supervisor and an Assistant Special Agent in Charge, both of whom report to the Special Agent in Charge. Division Counsel also report to the Special Agents in Charge of the field offices in which they work, not to the Office of the General Counsel at FBI Headquarters.

We found that these factors have led some Division Counsel to be reluctant to question the predication for NSL requests or the relevance of the information sought in the NSL to the investigation. The impact of these

factors on the independence and aggressiveness of Division Counsels' review of NSLs was manifest in an informal survey of 22 Chief Division Counsel who were asked by a Chief Division Counsel whether they would approve a particular NSL request. Some said that they would have approved the request for reasons other than the merits of the approval documentation. The results of this inquiry led senior attorneys in FBI-OGC's National Security Law Branch to be very concerned that some Chief Division Counsel believe they cannot exercise their independent professional judgment on the use of NSL authorities because they are reluctant to second guess the operational judgments of senior field office officials in their chain of command.

D. The OGC Database Does Not Identify the Targets of National Security Letters When They are Different From the Subjects of the Underlying Investigations

In our evaluation of the use and effectiveness of national security letters, we attempted to analyze information in the OGC database, including the numbers and types of NSL requests issued during the period of our review. One of the most significant Patriot Act expansions of NSL authorities was the lower predication standard of "relevance" to an authorized investigation. In lieu of requiring individualized suspicion about an investigative subject, the FBI is now permitted to obtain records on other individuals, so long as the information is relevant to an authorized investigation. However, we found that the OGC database does not capture information on whether the target of the NSL is the subject of the underlying investigating or another individual. As a result, because the target of an NSL is frequently not the same person as the subject of the underlying investigation, the FBI does not know and cannot estimate the number of NSL requests relating to persons who are not investigative subjects.

In 2006, the FBI modified its guidance to require, with the exception of NSLs seeking subscriber information pursuant to the ECPA NSL statute, that agents indicate in the NSL approval EC whether the request is for a person other than the subject of the investigation or in addition to that subject, and to state the U.S. person or non-U.S. person status of those individuals.

In light of the Patriot Act's expansion of the FBI's authority to collect information about individuals who are not subjects of its investigations, we believe the OGC database should contain this information so that the issue is subject to internal and external oversight.

VI. OIG Conclusions and Recommendations

Our review found that the FBI's use of national security letters has grown dramatically since enactment of the Patriot Act in October 2001. The FBI issued approximately 8,500 NSL requests in CY 2000, the last full year

prior to passage of the Patriot Act. After the Patriot Act, the number of NSL requests increased to approximately 39,000 in 2003, approximately 56,000 in 2004, and approximately 47,000 in 2005. During the period covered by our review, the FBI issued a total of 143,074 NSL requests pursuant to national security letter authorities. The overwhelming majority of the NSL requests sought telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the ECPA NSL statute.

Most NSL requests (about 73 percent) occurred during counterterrorism investigations. About 26 percent of all NSL requests were issued during counterintelligence investigations, and less than 1 percent of the requests were generated during foreign computer intrusion cyber investigations. In addition, the use of national security letters in FBI counterterrorism investigations increased from approximately 15 percent of investigations opened during 2003 to approximately 29 percent of the counterterrorism investigations opened during 2005.

We found that the use of NSL requests related to "U.S. persons" and "non-U.S. persons" shifted during our 3-year review period. The percentage of requests generated from investigations of U.S. persons increased from about 39 percent of all NSL requests issued in 2003 to about 53 percent of all NSL requests during 2005.

It is important to note that these statistics, which were obtained from the FBI electronic database that tracks NSL usage, understate the total number of national security letter requests. We found that the OGC database is inaccurate and does not include all national security letter requests issued by the FBI. Because of inaccuracies in the OGC database, we compared data in this database to a sample of investigative files in four FBI field offices that we visited. Overall, we found approximately 17 percent more national security *letters* and 22 percent more national security letter *requests* in the case files we examined in four field offices than were recorded in the OGC database. As a result, we believe that the total number of NSL requests issued by the FBI is significantly higher than the FBI reported.

We also found the OGC database did not accurately reflect the status of investigative targets and that the Department's semiannual classified reports to Congress on NSL usage were also inaccurate. Specifically, the data provided in the Department's semiannual classified reports regarding the number of requests for records, the number of different persons or organizations that were the subjects of investigations in which records were requested, and the status of those individuals as "U.S. persons or organizations" and "non-U.S. persons or organizations" were all inaccurate. We found that 12 percent of the case files we examined did not accurately report the status of the target of the NSL as being a U.S. person or a non-U.S. person. In each of these instances, the FBI database indicated that the

subject was a non-U.S. person while the approval memoranda in the investigative file indicated the subject was a U.S. person or a presumed U.S. person.

With respect to the effectiveness of national security letters, FBI Headquarters and field personnel told us that they believe NSLs are indispensable investigative tools that serve as building blocks in many counterterrorism and counterintelligence investigations. National security letters have various uses, including obtaining evidence to support FISA applications for electronic surveillance, pen register/trap and trace devices, or physical searches; developing communication or financial links between subjects of FBI investigations and between those subjects and others; providing evidence to initiate new investigations, expand national security investigations, or enabling agents to close investigations; providing investigative leads; and corroborating information obtained by use of other investigative techniques.

FBI agents and analysts also use information obtained from national security letters, in combination with other information, to prepare analytical intelligence products for distribution within the FBI and to other Department components, and for dissemination to other federal agencies, Joint Terrorism Task Forces, and other members of the intelligence community. We found that information derived from national security letters is routinely shared with United States Attorneys' Offices pursuant to various Departmental directives requiring terrorism prosecutors and intelligence research specialists to be familiar with FBI counterterrorism investigations. However, because information derived from national security letters is not marked or tagged as such, it is impossible to determine when and how often the FBI provided information derived from national security letters to law enforcement authorities for use in criminal proceedings.

We determined that information obtained from national security letters is routinely stored in the FBI's Automated Case Support (ACS) system, Telephone Applications, IDW, and other databases. FBI personnel and Joint Terrorism Task Force members who have the appropriate clearances to use these databases would therefore have access to information obtained from national security letters.

Our review also examined instances of "improper or illegal use" of national security letters. First, our review examined possible national security letter violations that the FBI was required to report to the President's Intelligence Oversight Board (IOB). The FBI identified 26 possible violations involving the use of national security letter authorities from calendar years 2003 through 2005, of which 19 were reported to the IOB. These 19 involved the issuance of NSLs without proper authorization, improper requests under the statutes cited in the national security letters, and unauthorized collection of telephone or Internet e-mail transactional records. Of these 26 possible violations, 22 were the result of FBI errors,

while 4 were caused by mistakes made by recipients of the national security letters.

Second, in addition to the violations reported by the FBI, we reviewed documents relating to national security letters in a sample of FBI investigative files in four FBI field offices. In our review of 77 FBI investigative files, we found that 17 of these files – 22 percent – contained one or more violations relating to national security letters that were not identified by the FBI. These violations included infractions that were similar to those identified by the FBI and considered as possible IOB violations, but also included instances in which the FBI issued national security letters for different information than what had been approved by the field supervisor. Based on our review and the significant percentage of files that contained unreported violations (22 percent), we believe that a significant number of NSL violations are not being identified or reported by the FBI.

Third, we identified many instances in which the FBI obtained telephone toll billing records and subscriber information from 3 telephone companies pursuant to more than 700 "exigent letters" signed by personnel in the Counterterrorism Division without first issuing national security letters. We concluded that the FBI's acquisition of this information circumvented the requirements of the ECPA NSL statute and violated the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) and internal FBI policy. These actions were compounded by the fact that the FBI used the exigent letters in non-emergency circumstances, failed to ensure that there were duly authorized investigations to which the requests could be tied, and failed to ensure that NSLs were issued promptly after the fact pursuant to existing or new counterterrorism investigations. In addition, the exigent letters inaccurately represented that the FBI had already requested subpoenas for the information when, in fact, it had not.

Fourth, we determined that in two circumstances during 2003 though 2005 FBI Headquarters Counterterrorism Division generated over 300 national security letters from "control files" rather than from "investigative files" in violation of FBI policy. In these instances, FBI agents did not generate and supervisors did not approve documentation demonstrating that the factual predicate required by the Electronic Communications Privacy Act, the Attorney General's NSI Guidelines, and internal FBI policy had been established. When NSLs are issued from control files rather than from investigative files, internal and external reviewers cannot determine whether the requests are tied to investigations that established the required evidentiary predicate for issuing the national security letters.

Fifth, we examined FBI investigative files in four field offices to determine whether FBI case agents and supervisors adhered to FBI policies designed to ensure appropriate supervisory review of the use of national security letter authorities. We found that 60 percent of the investigative

files we examined contained one or more violations of FBI internal control policies relating to national security letters. These included failures to document supervisory review of national security letter approval memoranda and failures to include required information such as the authorizing statute, the status of the investigative subject, or the number or types of records requested in NSL approval memoranda. Moreover, because the FBI has no policy requiring the retention of signed copies of national security letters, we were unable to conduct a comprehensive audit of the FBI's compliance with its internal control policies and the statutory certifications required for national security letters.

Our review also describes several other "noteworthy facts or circumstances" identified in the review. For example, we found that the FBI has not provided clear guidance describing how case agents and supervisors should apply the Attorney General Guidelines' requirement to use the "least intrusive collection techniques feasible" in their use and sequencing of national security letters. In addition, we found confusion among FBI attorneys and communication providers over the meaning of the phrase "telephone toll billing records information" in the ECPA NSL statute. We also saw indications that some Chief Division Counsel and Assistant Division Counsel are reluctant to provide an independent review of national security letter requests because these attorneys report to the Special Agents in Charge whose field supervisors have already approved the underlying investigation.

Finally, in evaluating the FBI's use of national security letters it is important to note the significant challenges the FBI was facing during the period covered by our review and the major organizational changes it was undergoing. Moreover, it is also important to recognize that in most cases the FBI was seeking to obtain information that it could have obtained properly if it had it followed applicable statutes, guidelines, and internal policies. We also did not find any indication that the FBI's misuse of NSL authorities constituted criminal misconduct.

However, as described above, we found that the FBI used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies. In addition, we found that the FBI circumvented the ECPA NSL statute when it issued over 700 "exigent letters" to obtain telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs. Moreover, in a few other instances, the FBI sought or obtained information to which it was not entitled under the NSL authorities when it sought educational records through issuance of an ECPA NSL, when it sought and obtained telephone toll billing records in the absence of a national security investigation, when it sought and obtained consumer full credit reports in counterintelligence investigations, and when it sought and obtained financial records and telephone toll billing records without first issuing NSLs.

Based on our review, we believe the FBI needs to ensure that all national security letters are issued in accord with applicable statutes, guidelines, and policies. Therefore, to address the issues identified in our report we recommend that the FBI:

1. Require all Headquarters and field personnel who are authorized to issue national security letter to create a control file for the purpose of retaining signed copies of all national security letters they issue.

2. Improve the FBI-OGC NSL tracking database to ensure that it captures timely, complete, and accurate data on NSLs and NSL requests.

3. Improve the FBI-OGC NSL tracking database to include data reflecting NSL requests for information about individuals who are not the investigative subjects but are the targets of NSL requests.

4. Issue additional guidance to field offices that will assist in identifying possible IOB violations arising from use of national security letter authorities, such as (a) measures to reduce or eliminate typographical and other errors in national security letters so that the FBI does not collect unauthorized information; (b) best practices for identifying the receipt of unauthorized information in the response to national security letters due to third-party errors; (c) clarifying the distinctions between the two NSL authorities in the Fair Credit Reporting Act (15 U.S.C. §§ 1681u and 1681v); and (d) reinforcing internal FBI policy requiring that NSLs must be issued from investigative files, not from control files.

5. Consider seeking legislative amendment to the Electronic Communications Privacy Act to define the phrase "telephone toll billing records information."

6. Consider measures that would enable FBI agents and analysts to (a) label or tag their use of information derived from national security letters in analytical intelligence products and (b) identify when and how often information derived from NSLs is provided to law enforcement authorities for use in criminal proceedings.

7. Take steps to ensure that the FBI does not improperly issue exigent letters.

8. Take steps to ensure that, where appropriate, the FBI makes requests for information in accordance with the requirements of national security letter authorities.

9. Implement measures to ensure that FBI-OGC is consulted about activities undertaken by FBI Headquarters National Security Branch, including its operational support activities, that could generate requests for records from third parties that the FBI is authorized to obtain exclusively though the use of its national security letter authorities.

10. Ensure that Chief Division Counsel and Assistant Division Counsel provide close and independent review of requests to issue national security letters.

We believe that these recommendations, if fully implemented, can improve the accuracy of the reporting of the FBI's use of national security letters and ensure the FBI's compliance with the requirements governing their use.