AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE INSPECTOR GENERAL'S INDEPENDENT REPORT ON THE FBI'S USE OF NATIONAL SECURITY LETTERS

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MARCH 20, 2007

Serial No. 110–21

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

34–175 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota
[Vacant]

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*
JOSEPH GIBSON, *Minority Chief Counsel*

CONTENTS

MARCH 20, 2007

OPENING STATEMENT

	Page
The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary	1
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary	2
The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Member, Committee on the Judiciary	4
The Honorable Trent Franks, a Representative in Congress from the State of Arizona, and Member, Committee on the Judiciary	5
The Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary	6
The Honorable J. Randy Forbes, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary	6

WITNESSES

Mr. Glenn A. Fine, Inspector General, U.S. Department of Justice	
Oral Testimony	7
Prepared Statement	10
Ms. Valerie Caproni, General Counsel, Federal Bureau of Investigation	
Oral Testimony	215
Prepared Statement	219

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	272
Prepared Statement of the Honorable Linda T. Sánchez, a Representative in Congress from the State of California, and Member, Committee on the Judiciary	279
Response to Post-hearing questions from Glenn A. Fine, Inspector General, U.S. Department of Justice	281
Post-hearing questions posed to Valerie Caproni, General Counsel, Federal Bureau of Investigation, from Chairman John Conyers, Jr.	286
Letter from Richard C. Powers, Assistant Director, Office of Congressional Affairs, Federal Bureau of Investigation	289
Prepared Statement of Caroline Frederickson, Director, Washington Legislative Office, American Civil Liberties Union (ACLU)	290
Letter requesting additional information submitted to Valerie Caproni, General Counsel, Federal Bureau of Investigation	295
Press release by the Department of Justice from March 9, 2007, submitted by the Honorable Howard Coble, a Represenative in Congress from the State of North Carolina, and Member, Committee on the Judiciary	297
Article entitled "Official Alerted F.B.I. to Rules Abuse 2 Year Ago, Lawyer Says," *The New York Times,* submitted by the Honorable John Conyers, Jr.	299

THE INSPECTOR GENERAL'S INDEPENDENT REPORT ON THE FBI'S USE OF NATIONAL SECURITY LETTERS

TUESDAY, MARCH 20, 2007

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 9:40 a.m., in Room 2141, Rayburn House Office Building, the Honorable John Conyers, Jr. (Chairman of the Committee) presiding.

Present: Representatives Conyers, Berman, Boucher, Nadler, Scott, Watt, Lofgren, Jackson Lee, Waters, Delahunt, Sánchez, Cohen, Johnson, Schiff, Davis, Wasserman Schultz, Ellison, Smith, Sensenbrenner, Coble, Goodlatte, Chabot, Lungren, Keller, Issa, Forbes, King, Feeney, Franks, and Gohmert.

Staff Present: Perry Apelbaum, General Counsel and Staff Director; Robert Reed, Oversight Counsel; Joseph Gibson, Minority Chief Counsel; Caroline Lynch, Minority Counsel; Ameer Gopalani, Majority Counsel.

Mr. CONYERS. Good morning. The Committee will come to order.

We are here for a hearing on the Inspector General's Independent Report on the FBI's Use of National Security Letters.

Nearly 6 years ago, in the immediate aftermath of September 11th, the Department of Justice told us that they needed significantly enhanced authority, while promising the Members of this Committee in no uncertain terms that these new tools would be carefully and appropriately used. Two years ago, when the PATRIOT Act was reauthorized, they promised us there was not a single instance in which the law had been abused.

Now, to underscore the importance of the reasons that we are holding this hearing, many of us remember the times in the past when the power of our Government has been abused. One war led to the suspension of Habeas Corpus; in another war, the notorious Palma raids; in World War II, the internment of Japanese Americans; in the Vietnam War, secret spying and enemy lists. In my view, we are now in a period where we risk a continuation of these deplorable acts and effect genuine harm to the Constitution and to the rule of law.

One week ago, the Inspector General told us that the exact opposite was true of the promise that had been made that there was not a single instance, when the PATRIOT Act was being reauthorized, that the law had been abused.

One tool in particular, the National Security Letters, essentially secret subpoenas issued without any court review, was used repeatedly to invade the privacy of law-abiding Americans outside the law and proper legal process. This was a serious breach of trust. The Department had converted this tool into a handy shortcut to illegally gather vast amounts of private information while at the same time significantly underreporting its activities to Congress. We learned that the number of National Security Letter requests had increased from 8,500 in the year 2000 to in excess of 143,000 from the 3-year period between 2003 and 2005. The Department of Justice consistently provided inaccurate information to Congress concerning the National Security Letters, failing to identify at least 4,600 security letter requests to us. The security letters were routinely issued without proper authorization and outside statutory and regulatory requirements.

The Inspector General found that more than 60 percent of the investigatory files they looked at included one or more violations of FBI policy; but worse, the Inspector General found even more widespread abuses concerning the so-called Exigent Letters: that is, emergency requests for telephone and other data. An Exigent Letter, as opposed to a National Security Letter is meant to obtain information in an extreme emergency like a kidnapping when the Bureau has already sought subpoenas for the requested information. But the FBI issued these letters in nonemergencies as a means to bypass the requirements of the National Security Letter procedure, and so, as if it were not troubling enough, in many instances, the Bureau attempted to issue after the fact National Security Letters to cover their tracks on their use of Exigent Letters. The Inspector General specifically found that the Exigent Letters were ordinarily issued when there was no emergency present and very often when there was not even a pending investigation. More often than not, the letters were issued based on promises that subpoenas were in the process of being issued, when that was not the case and even though some subpoenas were never issued at all.

The Federal Bureau of Investigation made numerous factual misstatements in the letters which were frequently issued in violation of the statute as well as the Attorney General and FBI guidelines. The recordkeeping was so poor that it was impossible for the IG to document how and why all of these problems occurred, and what disturbs me most is that the abuse and misuse of these security letters is not an isolated instance. It appears to be a part of a pattern in which the Department of Justice has violated not only our trust but the very laws which they are charged with enforcing, and so from the approval of the notorious torture memos to warrantless, illegal surveillance to the wrongful smearing of able U.S. Attorneys, this Department of Justice has squandered its reputation for independence and integrity. The Attorney General needs to understand that with power comes responsibility and with authority must come accountability.

I would like now to turn to the distinguished gentleman from Texas, the Ranking Member of this Committee, Mr. Lamar Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Chairman, I appreciate your holding this hearing on the Inspector General's report on the FBI's use of National Security Let-

ters. The Inspector General should be commended for conducting a thorough audit as directed by Congress and the PATRIOT Act reauthorization. The report raises concerns as to the FBI's internal recordkeeping and guidelines for the use of NSLs and terrorism and espionage investigations. It is clear from the report that these deficiencies are the result of the poor implementation and administration of National Security Letter authority. In other words, the problem is enforcement of the law, not the law itself. Timely corrected measures by the FBI and effective oversight by the Justice Department and Congress will ensure proper use of this important law.

The Inspector General's report found that the FBI's database for tracking NSLs significantly underestimated the number of NSL requests, resulting in inaccurate reports to Congress on the FBI's use of NSLs. From 2003 to 2005, the FBI issued a total of 143,074 NSLs. This compares to 739 Exigent Letters to three telephone companies issued contrary to national security investigation guidelines. The Exigent Letters represent 1/200th of the National Security Letters issued. Although the use of these unauthorized letters is disconcerting, the FBI discontinued this practice last year. The Inspector General makes two other very important findings.

First, there is no evidence that anyone at the FBI intended to violate the law or internal policy. This is a significant finding because it confirms that FBI agents acted in good faith and sought to comply with the law even as they worked under severe time constraints and with an urgent desire to thwart terrorist activities.

Second, as detailed by the Inspector General, NSLs are a critical tool in fighting terrorism and in keeping our country safe. The information acquired through NSLs is valuable to international terrorism and espionage investigations and has allowed the FBI and intelligence agencies to identify terrorists and spies, the sources of their financing and their plans to attack or harm our national security.

In addition, the FBI shares important information gathered through NSLs with other intelligence agencies, joint terrorism task forces and State and local law enforcement agencies. To do their job, the FBI must be able to collect important information about suspected terrorist and spies while complying with the law and freely share such information with key partners.

In response to extensive oversight efforts conducted last Congress, the PATRIOT Reauthorization Act added critical new safeguards. For instance, an NSL recipient can challenge the request in court. Nondisclosure orders require supervisory approval, and the recipient may disclose the NSL to an attorney. I applaud the Administration's response to the Inspector General's report and expect the Administration to follow through on its promise to act quickly to remedy the deficiencies identified by the Inspector General.

Mr. Chairman, on September 11, 2001, the United States was attacked. More than 3,000 people lost their lives. Members of Congress overwhelmingly approved important new counterterrorism tools for our Nation's law enforcement personnel and updated existing authorities to meet the terrorist threat. We must continue to demonstrate responsible leadership on the NSLs and other impor-

tant national security issues. Of course, we need to be vigilant to make sure these problems are fixed, that the Inspector General's recommendations are implemented and that our civil liberties and privacy are protected.

Mr. Chairman, I yield back the balance of my time.

Mr. CONYERS. I thank the gentleman for his statement.

I would like now to recognize the Chairman of the Constitution Subcommittee, Jerry Nadler, for 2½ minutes.

Mr. NADLER. I thank the Chairman. I would like to thank Chairman Conyers for holding this important hearing on the FBI abuses of National Security Letters.

We are here today in response to the Department of Justice Inspector General report that found widespread abuses of the FBI's authority to issue National Security Letters. An NSL can be issued to a third party such as a health insurance company or an Internet service provider, ordering them to reveal all of their information about you and your transactions, and the third party is prohibited from telling you or anyone else about the order. That is the so-called "gag order provision" so you cannot object to an NSL directed at your information in court as you could to a subpoena, because you do not know about it and the third party may have no interest in going to court to protect your rights or your privacy.

While last year's reauthorization of the PATRIOT Act did make some changes to the NSL provisions, these changes were essentially meaningless. For example, the court is now authorized to modify and set aside the gag order only if it finds there is no reason to believe that disclosure would endanger national security, diplomatic relations or anyone's life or safety, but the court must accept the Government's assertion of harm as conclusive, so this protection is meaningless.

Some of us had predicted that the unrestricted authority of the FBI to issue NSLs would be abused, and unfortunately, our worst fears have now been realized. The IG's NSLs have been used by the FBI to collect and retain private information about American citizens who are not reasonably suspected of being involved in terrorism. During the last Congress, we predicted that unchecked power would lead to rampant abuse. That is why I proposed the Stop Self-Authorized Secret Searches Act 2 years ago. This bill would have restored some pre-PATRIOT Act provisions that an NSL could not be issued unless the FBI made a factual, individualized showing that the records sought pertained to a suspected terrorist or spy. It would have given the recipient of a National Security Letter an opportunity to obtain legal counsel, the right to challenge the letter and the nondisclosure requirement, a real right to challenge it. It would have given notice to the target of the NSL if the Government later seeks to use the records obtained from the NSL against him or her in a subsequent proceeding. It would have given the target an opportunity to receive legal counsel and challenge the use of those records.

The bill would also have authorized the FBI to obtain documents that it legitimately needs while protecting the privacy of law-abiding American citizens.

The abuses by the DOJ and by the FBI have proven that these legislative fixes are a necessary check on the investigatory power.

We do not trust Government always to be run by angels, especially not this Administration. It is not enough to mandate that the FBI fix internal management problems in recordkeeping because the statute itself authorizes the unchecked selection of information on innocent Americans. Congress must act now to fix the statute authorizing the abuses revealed in the IG report and to hold those responsible for these abuses and violations accountable.

Thank you. I yield back.

Mr. CONYERS. Thank you.

The Chair recognizes the distinguished gentleman from Arizona, the Ranking minority Member of the Constitution Subcommittee, Trent Franks, for 2½ minutes.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Mr. Chairman, today our task is a vital one, to check and balance our sister branch of Government through oversight and to ensure citizens' rights are being properly safeguarded. Today's subject is somewhat delicate because we must all walk a fine line. In our great and critical responsibility to prevent jihadist attacks upon American citizens, we must also be careful to strike the proper balance between vigilance and fighting the enemy on the one side of the scales and the preservation of citizens' rights on the other.

The report of the Inspector General's that we review today is hopeful. We see that, while there are human imperfections in the FBI's operation, there is an overall finding that the FBI is, indeed, carrying out its duties responsibly, there being no evidence of any intentional or deliberate act to violate the law. The NSLs are performing their vital function as a valuable tool in national security investigations.

To put today's hearing in perspective, we should keep in mind that the issuance of NSLs under the PATRIOT Act is a relatively new process given that the PATRIOT Act is only a few years old and that this new use of NSLs will necessarily require a careful examination of their best and most appropriate use in this early period. Certainly, we will have to work out the kinks given that we are most likely in the business of fighting terror for a long time to come.

While the FBI's practices have had their shortcomings, it appears that these are problems that can be easily resolved, and this is good news. Many of the issues that we must review today are administrative in nature and, to some extent, unavoidable. Government is a human institution, and it is therefore by definition imperfect. Those of us who have run corporations know that a perfect audit is a very rare occurrence, particularly on the first go-around.

Most businesses do internal audits, perhaps many, many internal audits, to discover where human judgment has fallen short and where to improve before being audited by an outside source. This is an arduous but necessary task and one that I hope we do well here today and prospectively. The FBI has vowed that it will make all of the adjustments that Mr. Gonzalez and Ms. Caproni have recommended. We look forward to the realization of this goal.

With that, I thank the witnesses for joining us today, and we look forward to hearing your testimony.

Thank you, Mr. Chairman.

Mr. CONYERS. Thank you.

The Chair recognizes the distinguished gentleman from Virginia, Bobby Scott, Chairman of the Crime Subcommittee, for 2½ minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Chairman, we all believe that it is important to be aggressive in fighting terrorism and also aggressive in maintaining privacy and freedoms, and I do not believe we should operate on the premise that we always have to give up freedom in order to obtain security, but for us to provide appropriate oversight we have to have accurate information. Unfortunately, there are indications that we have received clearly inaccurate reports after the significant use of secret, invasive processes that do not appear to be necessary to advance terrorism-related investigations. Whether it is a secret NSA wiretapping in violation of the FISA law or the inappropriate use of the National Security Letters, we are discovering that what is actually occurring is quite different from what we were being told, and we cannot evaluate the ongoing need for NSA letters without accurate information.

There is also a clear indication of intentional misuse of the word "exigent" letters to telephone companies as emergency information when in fact no emergency existed. Somebody obviously knew that was a problem that would affect reports to Congress and oversight boards, and we need to find out who these people are. With these disturbing indications, Mr. Chairman, I hope the testimony of the witnesses today will reveal who is responsible for these abuses and who should be held accountable for false reports to Congress.

Thank you, Mr. Chairman. I yield back.

Mr. CONYERS. Thank you so much.

Another Virginian, the Ranking minority Member of the Crime Subcommittee, Mr. Randy Forbes.

Mr. FORBES. Mr. Chairman, I would like to thank you and the Ranking Member, Congressman Smith, for holding this important hearing today, and also for our witnesses for being here.

You know, the subject matter of this hearing makes for great theater, but when the show is over we have the task of finding the facts and making sure the proper balance is struck and implemented to protect our citizens. That we will do, and hopefully, we will do it without the negativism and the emotionalism that seems so prevailing in public policy today. Pounding our fists makes great sound bites, but does not stop terrorists or protect the privacy rights of our citizens.

It is clear that National Security Letters are important tools in international terrorism and espionage investigations conducted by the FBI. The Inspector General's report, which details the audit of 77 case files in four field offices, shows a disturbing pattern. In 60 percent of those cases, the FBI's files were found to be in violation of the FBI's internal control policies for issuing National Security Letters. While the audit conducted concluded that there was no evidence of any intentional or deliberate act to violate the law, it is also clear that changes need to be made to the FBI's procedures so that they reflect the scope and intent of the law rather than the evolution of general practice.

I look forward to hearing from the FBI about what procedures were in place during the time of the Inspector General's audit and

how, given the inadequacies identified by the Inspector General, the FBI plans to correct these.

Mr. Chairman, I yield back the balance of my time.

Mr. CONYERS. Thank you.

All other opening statements will be included in the record.

Mr. Glenn A. Fine, Inspector General at the Department of Justice, a post held since he was confirmed by the Senate on December 15, 2000. Mr. Fine has worked for the Department's Office of Inspector General in a variety of capacities since January 1995. He has had several years in private practice and has also served as an Assistant United States Attorney in Washington, D.C.

We are also privileged to have with us the General Counsel of the Federal Bureau of Investigation, Ms. Valerie Caproni, a position she has held since August 2003. Prior to that, Ms. Caproni served as an Assistant United States Attorney in the Eastern District of New York, as a supervisor at the Securities and Exchange Commission and has also worked in private practice.

All of your statements will be made a part of the record in their entirety, and we will have a 5-minute time for each of you, and we ask Inspector General Glenn A. Fine to begin our testimony.

Welcome to the Committee.

TESTIMONY OF GLENN A. FINE, INSPECTOR GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. FINE. Mr. Chairman, Congressman Smith and Members of the Committee on the Judiciary, thank you for inviting me to testify about two reports issued by the Department of Justice Office of the Inspector General regarding the FBI's use of National Security Letters and its use of section 215 orders to obtain business records.

The PATRIOT Reauthorization Act required the OIG to examine the FBI's use of these authorities, and on March 9th we issued reports detailing our findings. Today, I will summarize the key findings from our reviews, focusing my comments on the National Security Letter report.

Under five statutory provisions, the FBI can use National Security Letters (NSLs), to obtain without review by a court records such as customer information from telephone companies, Internet service providers, financial institutions, and consumer credit companies. Although most of the statutory provisions regarding NSLs existed prior to the enactment of the PATRIOT Act, the Act significantly broadened the FBI's authority to use NSLs in two primary ways.

First, it eliminated the requirement that the information sought must pertain to a foreign power or an agent of a foreign power and substituted the standard that the information requested must be relevant to or sought for an investigation to protect against international terrorism or espionage.

Second, the PATRIOT Act significantly expanded approval authority for NSLs beyond a limited number of FBI headquarters officials to the heads of all FBI field offices. Our review examined the FBI's use of NSLs from 2003 through 2005. The OIG will conduct another review examining the FBI's use of NSLs in 2006, which we are required to issue by the end of this year.

In sum, our review found widespread and serious misuse of the FBI's National Security Letter authorities. In many instances, the FBI's misuse violated NSL statutes, Attorney General guidelines, or the FBI's own internal policies. We also found that the FBI did not provide adequate guidance, adequate controls, or adequate training on the use of these sensitive authorities. Before describing the main findings of our report, however, I believe it is important to provide context for these findings.

First, we recognize the significant challenges the FBI was facing during the period covered by our review. After the September 11th terrorist attacks, the FBI implemented major organizational changes while responding to continuing terrorist threats and conducting many counterterrorism investigations, both internationally and domestically.

Second, it is also important to recognize that in most but not all of the cases we examined, the FBI was seeking information that it could have obtained properly through National Security Letters if it had followed applicable statutes, guidelines and internal policies.

Third, we did not find that the FBI employees sought to intentionally misuse NSLs or sought information that they knew they were not entitled to obtain. Instead, we believe the misuses and the problems we found generally were the product of mistakes, carelessness, confusion, sloppiness, lack of training, lack of adequate guidance, and lack of adequate oversight. I do not believe that any of my observations, however, excuses the FBI's misuse of National Security Letters.

When the PATRIOT Act enabled the FBI to obtain sensitive information through NSLs on a much larger scale, the FBI should have established sufficient controls and oversight to ensure the proper use of those authorities. The FBI did not do so. The FBI's failures, in my view, were serious and unacceptable.

I would now like to highlight our review's main findings. Our review found that after enactment of the PATRIOT Act the FBI's use of National Security Letters increased dramatically. In 2000, the last full year prior to the passage of the PATRIOT Act, the FBI issued approximately 8,500 NSL requests. 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. In total, during the 3-year period, the FBI issued more than 143,000 NSL requests. However, we believe that these numbers, which are based on information from the FBI's database, significantly understate the total number of NSL requests. During our file reviews in four FBI field offices, we found additional NSL requests in the files than were contained in the FBI database. In addition, many NSL requests were not included in the Department's reports to Congress.

Our review also attempted to assess the effectiveness of National Security Letters. NSLs have various uses, including to develop links of subjects of FBI investigations and other individuals and to provide leads and evidence to allow FBI agents to initiate or close investigations. Many FBI headquarters and field personnel, from agents in the field to senior officials, told the OIG that NSLs are indispensable investigative tools in counterterrorism and counter-

intelligence investigations, and they provided us with examples and evidence of the importance to these investigations.

The OIG review also examined whether there were any improper or illegal uses of NSL authorities. From 2003 through 2005, the FBI identified 26 possible intelligence violations involving its use of NSLs. We visited four FBI field offices and reviewed a sample of 77 investigative case files and 293 NSLs. We found 22 possible violations that had not been identified or reported by the FBI. We have no reason to believe that the number of violations we identified in the field offices was skewed or disproportionate to the number of violations in other files. This suggests that the large number of NSL-related violations throughout the FBI have not been identified or reported by FBI personnel.

In one of the most troubling findings, we determined that the FBI improperly obtained telephone toll billing records and subscriber information from three telephone companies pursuant to over 700 so-called Exigent Letters. These letters generally were signed by personnel in the Communications Analysis Unit (CAU), a unit of the Counterterrorism Division in the FBI Headquarters. The Exigent Letters were based on a form letter used by the FBI's New York Field Division in the criminal investigations related to the September 11th attacks.

Our review found that the FBI sometimes used these Exigent Letters in nonemergency circumstances. In addition, the FBI failed to ensure that there were authorized investigations to which the requests could be tied. The Exigent Letters also inaccurately represented that the FBI had already requested subpoenas for the information when in fact it had not. The FBI also failed to ensure that NSLs were issued promptly to telephone companies after the Exigent Letters were sent. Rather, in many instances, after obtaining records from the telephone companies, the FBI issued National Security Letters months after the fact to cover the information obtained.

We concluded that the FBI's use of these Exigent Letters inappropriately circumvented the requirements of the NSL statute and violated Attorney General guidelines and FBI policies. In response to our report, we believe that the Department and the FBI are taking our findings seriously. The FBI concurred with all of our recommendations, and the Department's National Security Division will be actively engaged in oversight of the FBI's use of NSLs.

In addition, the FBI's Inspection Division has initiated audits of a sample of NSLs issued by each of its 56 field offices. The FBI is also conducting a special investigation on the use of Exigent Letters to determine how and why the problems occurred. The OIG will continue to review the FBI's use of National Security Letters. In addition to issuing a second report on the use of NSLs in 2006, we intend to monitor the actions that the FBI and the Department are taking to address the problems we found in that review.

Finally, I want to note that the FBI and the Department cooperated fully with our reviews, agreed to declassify information in the report, and appears to be committed to addressing the problems we identified. We believe that significant efforts are necessary to ensure that the FBI's use of National Security Letters is conducted

in full accord with the statutes, Attorney General guidelines, and FBI policy.

That concludes my testimony, and I will be pleased to answer any questions.

[The prepared statement of Mr. Fine follows:]

PREPARED STATEMENT OF GLENN A. FINE

Mr. Chairman, Mr. Smith, and members of the Committee on the Judiciary:

Thank you for inviting me to testify about two recent reports issued by the Department of Justice Office of the Inspector General (OIG) regarding the Federal Bureau of Investigation's (FBI) use of national security letters and the FBI's use of Section 215 orders to obtain business records. In the Patriot Reauthorization Act, enacted in 2006, Congress directed the OIG to examine the FBI's use of these two important authorities. The reviews were directed to examine, among other things, the number of times these authorities were used, the importance of the information obtained, how the information was utilized, any improper or illegal uses of these authorities, and other noteworthy facts or circumstances related to their use.

On March 9, 2007, we issued separate reports on the FBI's use of national security letters and Section 215 orders. We publicly released two unclassified reports, with only limited information redacted (blacked out) which the Department or the FBI considered to be classified. We also provided to Congress, including this Committee, copies of the full classified reports that contain some additional classified information on the FBI's use of the two authorities. However, the OIG's main findings and conclusions are included in the unclassified versions that were publicly released.

In this written statement, I will summarize the key findings from our reports, focusing most of my comments on the national security letters report. I will first provide brief background on national security letters and how we conducted our review. I will then provide a few observations to put our findings in context. Next, I will highlight the main findings of our national security letter report. After that, I will briefly summarize our report on the FBI's use of Section 215 orders to obtain business records.

I. THE OIG'S NATIONAL SECURITY LETTER REPORT

A. Background on National Security Letters

Under five statutory provisions, the FBI can use national security letters (NSLs) to obtain—without a court order or any review by a court—records such as customer information from telephone companies, Internet service providers, financial institutions, and consumer credit companies. Most of these statutory provisions regarding NSLs existed prior to enactment of the USA PATRIOT Act (Patriot Act) in October 2001. Prior to the Patriot Act, the FBI could obtain information using a national security letter only if it had "specific and articulable facts giving reason to believe that the customer or entity whose records are sought [was] a foreign power or agent of a foreign power." In addition, NSLs could only be issued by a limited number of senior FBI Headquarters officials.

The Patriot Act significantly broadened the FBI's authority to use NSLs by both lowering the threshold standard for issuing them and by expanding the number of FBI officials who could sign the letters. First, the Patriot Act eliminated the requirement that the information sought must pertain to a foreign power or an agent of a foreign power. Instead, it substituted the lower threshold standard that the information requested must be relevant to or sought for an investigation to protect against international terrorism or espionage. Consequently, the Patriot Act authorized the FBI to issue national security letters to request information about persons other than the subjects of FBI national security investigations, so long as the requested information is relevant to an authorized national security investigation.

In addition, the Patriot Act permitted Special Agents in Charge of the FBI's 56 field offices to sign national security letters, which significantly expanded approval authority beyond a limited number of FBI Headquarters officials. Finally, the Patriot Act added a new authority allowing NSLs to be used to obtain consumer full credit reports in international terrorism investigations.

B. The OIG Review

As directed by the Patriot Reauthorization Act, the OIG's report examined the FBI's use of national security letters during the time period from 2003 through 2005. As required by the Reauthorization Act, the OIG will conduct another review

examining the use of NSLs in 2006, which we are required to issue by the end of this year.

During our review, a team of OIG staff conducted interviews of over 100 FBI and Department of Justice employees, including personnel at FBI Headquarters, the FBI Office of the General Counsel (OGC), FBI Counterterrorism and Counterintelligence Divisions, FBI personnel in four field divisions, and officials in the Department's Criminal Division.

In addition, the OIG reviewed a sample of FBI case files that contained national security letters at four FBI field divisions: Chicago, New York, Philadelphia, and San Francisco. These field divisions were selected from among the eight FBI field divisions that issued the most NSL requests during the review period. During our field work at the four field divisions, we examined a sample of 77 investigative case files that contained 293 national security letters. An investigative case file can contain a large number of documents, and some of the case files we reviewed consisted of the equivalent of 20 or 30 boxes of documents. We used a judgmental sample in selecting which files to review and included in our sample both counterterrorism and counterintelligence cases, cases in which the NSLs were issued during preliminary investigations and full investigations, and opened and closed FBI cases.

The OIG also analyzed the FBI OGC's national security letter tracking database, which the FBI uses for collecting information to compile the Department's required reports to Congress on NSL usage. Finally, we distributed an e-mail questionnaire to the counterintelligence and counterterrorism squads in the FBI's 56 field divisions in an effort to determine the types of analytical products the FBI developed based on NSLs, the manner in which NSL-derived information was disseminated, and the occasions when such information was provided to law enforcement authorities for use in criminal proceedings.

C. Findings of the OIG Review

Our review found widespread and serious misuse of the FBI's national security letter authorities. In many instances, the FBI's misuse of national security letters violated NSL statutes, Attorney General Guidelines, or the FBI's own internal policies. We also found that the FBI did not provide adequate guidance, adequate controls, or adequate training on the use of these sensitive authorities. In many respects, the FBI's oversight of the use of NSL authorities expanded by the Patriot Act was inconsistent and insufficient.

1. Background to OIG Findings

However, before detailing the main findings of our report, I believe it is important to provide context for these findings and also to note what our review did not find.

First, in evaluating the FBI's misuse of national security letters, it is 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 prevent additional terrorist attacks in the United States. These changes included overhauling and expanding its counterterrorism operations, expanding its intelligence capabilities, attempting 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 had to respond to continuing terrorist threats and conduct many counterterrorism investigations, both internationally and domestically.

Second, it is important to recognize that in most—but not all—of the cases we examined in this review, the FBI was seeking information that it could have obtained properly through national security letters if it had followed applicable statutes, guidelines, and internal policies.

Third, national security letters are important tools that can provide critical evidence in counterterrorism and counterintelligence investigations. Many Headquarters and field personnel—from agents to senior officials—believe these tools are indispensable to the FBI's mission to detect and deter terrorism and espionage.

Fourth, we did not find that that FBI agents sought to intentionally misuse the national security letters or sought information that they knew they were not entitled to obtain through the letters. Instead, we believe the misuses and the problems we found were the product of mistakes, carelessness, confusion, sloppiness, lack of training, lack of adequate guidance, and lack of adequate oversight.

Yet, I do not believe that any of these observations excuse the FBI's widespread and serious misuse of its national security letter authorities. When the Patriot Act enabled the FBI to obtain sensitive information through NSLs on a much larger scale, the FBI should have established sufficient controls and oversight to ensure the proper use of these authorities. The FBI did not do so. The FBI's failures, in my view, were serious and unacceptable.

I would now like to highlight our review's main findings, which are detailed in the OIG's 126-page report.

2. OIG Findings

Our review found that, after enactment of the Patriot Act, the FBI's use of national security letters increased dramatically. In 2000, the last full year prior to passage of the Patriot Act, the FBI issued approximately 8,500 NSL requests. It is important to note that one national security letter may request information about multiple telephone numbers or e-mail addresses. Because the FBI's semiannual classified reports to Congress provide the number of requests rather than the number of letters, we also focused on the total number of requests.

After the Patriot Act, the number of NSL requests issued by the FBI increased to approximately 39,000 in 2003, approximately 56,000 in 2004, and approximately 47,000 in 2005. In total, during the 3-year period covered by our review, the FBI issued more than 143,000 NSL requests.

However, we believe that these numbers, which are based on information from the FBI's database, understate the total number of NSL requests issued by the FBI. During our review, we found that the FBI database used to track these requests is inaccurate and does not include all NSL requests.

First, when we compared information from the database to the documents contained in investigative case files in the 4 FBI field offices that we visited, we found approximately 17 percent more NSL letters and 22 percent more NSL requests in the case files than we could find in the FBI database. In addition, we determined that many NSL requests were not included in the Department's reports to Congress because of the FBI's delays in entering NSL information into its database. We also found problems and incorrect data entries in the database that caused NSLs to be excluded from the Department's reports to Congress.

Therefore, based on shortcomings in the FBI's NSL database and its reporting processes, we concluded that the Department's semiannual classified reports to Congress on NSL usage were inaccurate and significantly understated the total number of NSL requests during the review period.

Our report also provides breakdowns on the types of NSLs used by the FBI. We determined that, overall, approximately 73 percent of the total number of NSL requests were used in counterterrorism investigations and 26 percent in counterintelligence cases.

In addition, our review found that the percentage of NSL requests that related to investigations of U.S. persons increased from about 39 percent of all NSL requests in 2003 to about 53 percent in 2005.

As directed by the Patriot Reauthorization Act, our review attempted to assess the effectiveness of national security letters. NSLs have various uses, including to develop evidence to support applications for orders issued under the Foreign Intelligence Surveillance Act (FISA), develop links between subjects of FBI investigations and other individuals, provide leads and evidence to allow FBI agents to initiate or close investigations, and corroborate information obtained by other investigative methods. FBI personnel told the OIG that NSLs are indispensable investigative tools in many counterterrorism and counterintelligence investigations, and they provided us with examples and evidence of their importance to these investigations.

We determined that information obtained from NSLs is also used in FBI analytical intelligence products that are shared within the FBI and with DOJ components, Joint Terrorism Task Forces, other federal agencies, and other members of the intelligence community.

In addition, information obtained from NSLs is stored in FBI databases such as its Automated Case Support system and its Investigative Data Warehouse. However, because information is not tagged or identified in FBI files or databases as derived from NSLs, we could not determine the number of times that NSLs were used in such analytical products, shared with other agencies, or used in criminal cases.

As also directed by the Patriot Reauthorization Act, the OIG review examined whether there were any "improper or illegal uses" of NSL authorities. We found that from 2003 through 2005, the FBI identified 26 possible intelligence violations involving its use of NSLs, 19 of which the FBI reported to the President's Intelligence Oversight Board (IOB). Of the 26 possible violations, 22 were the result of FBI errors, while 4 were caused by mistakes made by recipients of the NSLs.

These possible violations included the issuance of NSLs without proper authorization, improper requests under the statutes cited in the NSLs, and unauthorized collection of telephone or Internet e-mail transactional records. For example, in three of these matters the FBI obtained the information without issuing national security letters. One of these three matters involved receipt of information when there was no open national security investigation. In another matter, the FBI issued national

security letters seeking consumer full credit reports in a counterintelligence investigation, which the NSL statutes do not permit. In other matters, the NSL recipient provided more information than was requested in the NSL, or provided information on the wrong person, either due to FBI typographical errors or errors by the recipients of NSLs.

In addition to the possible violations reported by the FBI, we reviewed FBI case files in four field offices to determine if there were unreported violations of NSL authorities, Attorney General Guidelines, or internal FBI policies governing the approval and use of NSLs. Our review of 293 national security letters in 77 files found 22 possible violations that had not been identified or reported by the FBI.

The violations we found fell into three categories: improper authorization for the NSL, improper requests under the pertinent national security letter statutes, and unauthorized collections. Examples of the violations we identified include issuing NSLs for consumer full credit reports in a counterintelligence case, which is not statutorily permitted; issuing an NSL for a consumer full credit report when the FBI Special Agent in Charge had approved an NSL for more limited credit information under a different NSL authority; issuing an NSL when the investigation had lapsed; and obtaining telephone toll billing records for periods in excess of the time period requested in the NSL due to third-party errors.

Thus, it is significant that in the limited file review we conducted of 77 investigative files in 4 FBI field offices, we identified nearly as many NSL-related violations (22) as the total number of possible violations that the FBI had identified (26) in reports from all FBI Headquarters and field divisions over the entire 3-year period. Moreover, 17 of the 77 files we reviewed, or 22 percent, had 1 or more violations.

We have no reason to believe that the number of violations we identified in the four field offices we visited was skewed or disproportionate to the number of possible violations in other files. This suggests that a large number of NSL-related violations throughout the FBI have not been identified or reported by FBI personnel.

Our examination of the violations we identified did not reveal deliberate or intentional violations of the NSL statutes, the Attorney General Guidelines, or FBI policy. We believe that some of these violations demonstrated FBI agents' confusion and unfamiliarity with the constraints on national security letter authorities. We also believe that many of the violations occurred because FBI personnel do not consistently cross check the NSL approval documentation with the proposed NSLs, or verify upon receipt that the information supplied by the recipient matches the request. Other violations demonstrated inadequate supervision over use of these authorities.

We examined the FBI investigative files in the four field offices to determine whether FBI case agents and supervisors had adhered to FBI policies designed to ensure appropriate supervisory review of the use of NSL authorities. We found that 60 percent of the investigative files we examined contained one or more violations of FBI internal policies relating to national security letters. These included failures to document supervisory review of NSL approval memoranda and failures to include in NSL approval memoranda required information, such as the authorizing statute, the status of the investigative subject, or the number or types of records requested.

In another finding, our review determined that the FBI Headquarters Counterterrorism Division generated over 300 NSLs exclusively from "control files" rather than from "investigative files," in violation of FBI policy. When NSLs are issued from control files, the NSL documentation does not indicate whether the NSLs are issued in authorized investigations or whether the information sought in the NSLs is relevant to those investigations. This documentation is necessary to establish compliance with NSL statutes, Attorney General Guidelines, and FBI policies.

In addition, we found that the FBI had no policy requiring the retention of signed copies of national security letters. As a result, we were unable to conduct a comprehensive audit of the FBI's compliance with its internal control policies and the statutory certifications required for NSLs.

In one of the most troubling findings, we determined that from 2003 through 2005 the FBI improperly obtained telephone toll billing records and subscriber information from 3 telephone companies pursuant to over 700 so-called "exigent letters." These letters generally were signed by personnel in the Communications Analysis Unit (CAU), a unit of the Counterterrorism Division in FBI Headquarters, and were based on a form letter used by the FBI's New York Field Division in the criminal investigations related to the September 11 attacks. The exigent letters signed by the CAU typically 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.

These letters were signed by CAU Unit Chiefs, CAU special agents, and subordinate personnel, none of whom were delegated authority to sign NSLs.

Our review found that that the FBI sometimes used these exigent letters in non-emergency circumstances. In addition, the FBI failed to ensure that there were duly authorized investigations to which the requests could be tied. The exigent letters also inaccurately represented that the FBI had already requested subpoenas for the information when, in fact, it had not. The FBI also failed to ensure that NSLs were issued promptly to the telephone companies after the exigent letters were sent. Rather, in many instances, after obtaining records from the telephone companies the FBI issued national security letters many months after the fact to "cover" the information obtained.

As our report describes, we were not convinced by the legal justifications offered by the FBI during our review for the FBI's acquisition of telephone toll billing records and subscriber information in response to the exigent letters without first issuing NSLs. The first justification offered was the need to reconcile the strict requirements of the NSL statute with the FBI's mission to prevent terrorist attacks. While the FBI's counterterrorism mission may require streamlined procedures to ensure the timely receipt of information in genuine emergencies, the FBI needs to address the problem by expediting the issuance of national security letters or by seeking legislative modification to the voluntary emergency disclosure provision in the Electronic Communications Privacy Act (ECPA), not through these exigent letters. Moreover, the FBI's justification for the exigent letters was undercut because they were used in non-emergency circumstances, not followed in many instances within a reasonable time by the issuance of NSLs, and not catalogued in a fashion that would enable FBI managers or anyone else to review the practice or the predication required by the NSL statute.

In sum, we concluded that the FBI's use of these letters inappropriately circumvented the requirements of the NSL statute, and violated Attorney General Guidelines and FBI policies.

As directed by the Patriot Reauthorization Act, our report also describes several other "noteworthy facts or circumstances" we identified in the review. For example, we found that the FBI did not provide clear guidance describing how FBI case agents and supervisors should apply the Attorney General Guidelines' requirement to use the "least intrusive collection techniques feasible" during national security investigations to the use and sequencing of national security letters. In addition, we saw indications that some FBI lawyers in field offices were reluctant to provide an independent review of NSL requests because these lawyers report to senior field office managers who already had approved the underlying investigations.

D. Recommendations

To help the FBI address these significant findings, the OIG made a series of recommendations, including that the FBI improve its database to ensure that it captures timely, complete, and accurate data on NSLs; that the FBI take steps to ensure that it uses NSLs in full accord with the requirements of national security letter authorities; and that the FBI issue additional guidance to field offices that will assist in identifying possible violations arising from use of NSLs. The FBI concurred with all of the recommendations and agreed to implement corrective action.

We believe that the Department and the FBI are taking the findings of the report seriously. In addition to concurring with all our recommendations, the FBI and the Department have informed us that they are taking additional steps to address the problems detailed in the report. For example, the FBI's Inspection Division has initiated audits of a sample of NSLs issued by each of its 56 field offices. It is also conducting a special inspection of the exigent letters sent by the Counterterrorism Division to three telephone companies to determine how and why that occurred.

The FBI's Office of the General Counsel is also consolidating its guidance on NSLs, providing additional guidance and training to its field-based Chief Division Counsel on their role in approving NSLs, and working to develop a new web-based NSL tracking database.

In addition to the FBI's efforts, we have been told that the Department's National Security Division will be actively engaged in oversight of the FBI's use of NSL authorities.

As required by the Patriot Reauthorization Act, the OIG will continue to review the FBI's use of national security letters. We are required by the Act to issue another report by the end of this year on the FBI's use of NSLs in 2006. In addition, we intend to monitor the actions that the FBI and the Department have taken and are taking to address the problems we found in our first review.

II. THE OIG'S SECTION 215 REPORT

In the last section of my statement, I want to summarize briefly the OIG's second report, which examined the FBI's use of Section 215 orders to obtain business records. Section 215 of the Patriot Act allows the FBI to seek an order from the FISA Court to obtain "any tangible thing," including books, records, and other items, from any business, organization, or entity provided the item or items are for an authorized investigation to protect against international terrorism or clandestine intelligence activities.

Section 215 of the Patriot Act did not create new investigative authority, but instead significantly expanded existing authority found in FISA by broadening the types of records that could be obtained and by lowering the evidentiary threshold to obtain a Section 215 order for business records. Public concerns about the scope of this expanded Section 215 authority centered on the ability of the FBI to obtain library records, and many public commentators began to refer to Section 215 as the "library provision."

Our review found that the FBI and the Department's Office of Intelligence Policy and Review (OIPR) submitted to the FISA Court two different kinds of applications for Section 215 orders: "pure" Section 215 applications and "combination" Section 215 applications. A "pure" Section 215 application is a term used to refer to a Section 215 application for any tangible item which is not associated with an application for any other FISA authority. A "combination" Section 215 application is a term used to refer to a Section 215 request that was added to a FISA application for pen register/trap and trace orders, which identify incoming and outgoing telephone numbers called on a particular line. In a combination order, the Section 215 request was added to the pen register/trap and trace application in order to obtain subscriber information related to the telephone numbers.

We found that from 2002 through 2005 the Department, on behalf of the FBI, submitted to the FISA Court a total of 21 pure Section 215 applications and 141 combination Section 215 applications.

We found that the first pure Section 215 order was approved by the FISA Court in spring 2004, more than 2 years after enactment of the Patriot Act. The FISA Court approved six more pure Section 215 applications that year, for a total of seven in 2004. The FISA Court approved 14 pure Section 215 applications in 2005.

Examples of the types of business records that were obtained through pure Section 215 orders include driver's license records, public accommodations records, apartment records, and credit card records.

We also determined that the FBI did not obtain Section 215 orders for any library records from 2002 through 2005 (the time period covered by our review). The few applications for Section 215 orders for library records that were initiated in the FBI during this period were withdrawn while undergoing the review process within the FBI and the Department. None were submitted to the FISA Court.

With respect to how information from Section 215 orders was used, we found no instance where the information obtained from a Section 215 order resulted in a major case development such as disruption of a terrorist plot. We also found that very little of the information obtained in response to Section 215 orders has been disseminated to intelligence agencies outside the DOJ.

However, FBI personnel told us they believe that the kind of intelligence gathered from Section 215 orders is essential to national security investigations. They also stated that the importance of the information is sometimes not known until much later in an investigation, when the information is linked to some other piece of intelligence. FBI officials and Department attorneys also stated that they believe Section 215 authority is useful because it is the only compulsory process for certain kinds of records that cannot be obtained through alternative means.

We did not identify any instances involving "improper or illegal use" of a pure Section 215 order. We did find problems with two combination Section 215 orders. In one instance, the FBI inadvertently collected information from a telephone number that no longer belonged to the target of the investigation. In another instance, the FBI received information from a telephone that was no longer connected to the subject because of a mistake by the telephone company.

We also found that the FBI has not used Section 215 orders as effectively as it could have because of legal, bureaucratic, or other impediments to obtaining these orders. For example, after passage of the Patriot Act in October 2001, neither the Department nor the FBI issued implementing procedures or guidance with respect to the expansion of Section 215 authority for a long period of time. In addition, we found significant delays within the FBI and the Department in processing requests for Section 215 orders. We also determined through our interviews that FBI field offices do not fully understand Section 215 orders or the process for obtaining them.

III. CONCLUSION

In sum, our review of national security letters revealed that, in various ways, the FBI violated the national security letter statutes, Attorney General Guidelines, or FBI internal policies governing their use. While we did not find that the violations were deliberate, we believe the misuses were widespread and serious.

Finally, I also want to note that the FBI and the Department cooperated fully with our review. In addition, the FBI and the Department agreed to declassify important aspects of the report to permit a full and fair airing of the issues we describe in the report. They have also acknowledged the problems we found and have not attempted to cover up the deficiencies. The FBI and the Department also appear to be taking the findings of the report seriously, and appear committed to correcting the problems we identified.

We believe that these serious and ongoing efforts are necessary to ensure that the FBI's use of national security letter authorities to obtain sensitive information is conducted in full accord with the NSL statutes, Attorney General Guidelines, and FBI policies.

That concludes my testimony, and I would be pleased to answer any questions.

ATTACHMENT

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

A Review of the Federal Bureau of Investigation's Use of National Security Letters

Office of the Inspector General
March 2007

UNCLASSIFIED

TABLE OF CONTENTS

TABLE OF CONTENTS i

INDEX OF CHARTS, DIAGRAMS, AND TABLES vi

LIST OF ACRONYMS vii

EXECUTIVE SUMMARY viii

CHAPTER ONE: INTRODUCTION 1

I. Provisions of the USA Patriot Act and Reauthorization Act 1

II. Methodology of the OIG Review 3

III. Organization of the Report 5

CHAPTER TWO: BACKGROUND 7

I. Background on National Security Letters 7

A. The Patriot Act 8

B. Types of Information Obtained by National Security Letters 10

C. The Patriot Reauthorization Act 10

II. The Four National Security Letter Statutes 11

A. The Right to Financial Privacy Act 11

B. The Electronic Communications Privacy Act 12

C. The Fair Credit Reporting Act 14

D. The National Security Act 15

III. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection 16

A. Levels of Investigative Activity under the FCI Guidelines (January 1, 2003 – October 31, 2003) 16

B. Levels of Investigative Activity under the NSI Guidelines (October 31, 2003) 17

IV. The Role of FBI Headquarters and Field Offices in Issuing and Using National Security Letters 18

A. FBI Headquarters 18

1. Counterterrorism Division 19
2. Counterintelligence Division 19
3. Cyber Division 19
4. Directorate of Intelligence 19
5. Office of the General Counsel (FBI-OGC) 20
B. FBI Field Divisions 20
1. Chief Division Counsel 20
2. Field Intelligence Groups 21

CHAPTER THREE: THE FBI'S COLLECTION AND RETENTION OF INFORMATION OBTAINED FROM NATIONAL SECURITY LETTERS 22

I. The FBI's Process for Collecting Information Through National Security Letters 22

II. The FBI's Retention of Information Obtained from National Security Letters 27

CHAPTER FOUR: NATIONAL SECURITY LETTER REQUESTS ISSUED BY THE FBI FROM 2003 THROUGH 2005 31

I. Inaccuracies in the FBI's National Security Letter Tracking Database 31

II. National Security Letter Requests From 2003 Through 2005 36

CHAPTER FIVE: THE EFFECTIVENESS OF NATIONAL SECURITY LETTERS AS AN INVESTIGATIVE TOOL 42

I. Introduction 42

II. The Effectiveness of National Security Letters Prior to the Patriot Act 43

III. The Effectiveness of National Security Letters as an Investigative Tool in 2003 through 2005 45
A. The Importance of the Information Acquired From National Security Letters to the Department's Intelligence Activities 45
1. Principal Uses of National Security Letters 46
2. The Value of Each Type of National Security Letter 48

B. Analysis of Information Obtained From National Security Letters 52

1. Types of Analysis 52

2. Formal Analytical Intelligence Products 54

C. The FBI's Dissemination of Information Obtained From National Security Letters to Other Entities 56

D. Information From National Security Letters Provided to Law Enforcement Authorities for Use in Criminal Proceedings 60

1. Routine Information Sharing With United States Attorneys' Offices 60

2. Providing Information to Law Enforcement Authorities for Use in Criminal Proceedings 62

IV. Conclusion 65

CHAPTER SIX: IMPROPER OR ILLEGAL USE OF NATIONAL SECURITY LETTER AUTHORITIES 66

I. Possible IOB Violations Arising from National Security Letters Identified by the FBI 67

A. The IOB Process for Reporting Possible Violations of Intelligence Activities in the United States 68

B. Field Division Reports to FBI-OGC of 26 Possible IOB Violations Involving the Use of National Security Letters 69

1. Possible IOB Violations Identified by the FBI 69

2. OIG Analysis Regarding Possible IOB Violations Identified by the FBI 77

II. Additional Possible IOB Violations Identified by the OIG During Our Field Visits 78

A. Possible IOB Violations Identified by the OIG 78

B. National Security Letter Issued in a Charlotte, N.C. Terrorism Investigation 82

C. OIG Analysis Regarding Possible IOB Violations Identified or Reviewed by the OIG 84

III. Improper Use of National Security Letter Authorities by Units in FBI Headquarters' Counterterrorism Division Identified by the OIG 86

A. Using "Exigent Letters" Rather Than ECPA National Security Letters 86

1. FBI Contracts With Three Telephone Companies 87

2. The Exigent Letters to Three Telephone Companies 89

3. Absence of Investigative Authority for the Exigent Letters 92

4. Efforts by the FBI's National Security Law Branch to Conform CAU's Practices to the Electronic Communications Privacy Act 93

5. OIG Analysis of Exigent Letters 95

B. National Security Letters Issued From Headquarters Control Files Rather Than From Investigative Files 98

1. National Security Letters Issued From a Headquarters Special Project Control File 98

2. National Security Letters Issued by the Electronic Surveillance Operations and Sharing Unit 100

3. OIG Analysis 102

IV. Failure to Adhere to FBI Internal Control Policies on the Use of National Security Letter Authorities 103

1. Lapses in Internal Controls 104

2. OIG Analysis of Failures to Adhere to FBI Internal Control Policies 106

CHAPTER SEVEN: OTHER NOTEWORTHY FACTS AND CIRCUMSTANCES RELATED TO THE FBI'S USE OF NATIONAL SECURITY LETTERS 108

I. Using the "least intrusive collection techniques feasible" 108

II. Telephone "toll billing records information" 111

III. The Role of FBI Division Counsel in Reviewing National Security Letters 112

IV. Issuing NSLs From "Control Files" Rather Than From "Investigative Files" 115

V. Obtaining Records From Federal Reserve Banks in Response to "Certificate Letters" Rather Than by Issuing RFPA NSLs 115

VI. The OGC Database Does Not Identify the Targets of National Security Letters When They are Different From the Subjects of the Underlying Investigations 118

CHAPTER EIGHT: CONCLUSIONS AND RECOMMENDATIONS 120

INDEX OF CHARTS, DIAGRAMS, AND TABLES

		Page
Chart 1.1	Relationship Between NSLs and NSL Requests	4
Chart 4.1	NSL Requests (2003 through 2005)	37
Chart 4.2	NSL Requests Reported to Congress Relating to U.S. Persons and non-U.S. Persons (2003 through 2005)	38
Chart 4.3	NSL Requests in Counterterrorism, Counterintelligence, and Foreign Cyber Investigations (2003 through 2005)	39
Chart 4.4	Counterterrorism Investigations With One or More National Security Letters (2003 through 2005)	40
Chart 4.5	NSL Requests During Preliminary and Full Investigations Identified in Files Reviewed by OIG (2003 through 2005)	41
Diagram 5.1	How the FBI Uses National Security Letters	47
Table 6.1	Summary of 26 Possible IOB Violations Triggered by Use of National Security Letters Reported to FBI-OGC (2003 through 2005)	70
Table 6.2	Summary of 22 Possible IOB Violations Triggered by Use of National Security Letters Identified by the OIG in Four Field Offices	79

LIST OF ACRONYMS

ACS	Automated Case Support
ASAC	Assistant Special Agent in Charge
ATAC	Anti-Terrorism Advisory Council
CAU	Communications Analysis Unit
CDC	Chief Division Counsel
CXS	Communications Exploitations Section
CY	Calendar Year
DIDO	Designated Intelligence Disclosure Official
EAD	Executive Assistant Director
EC	Electronic Communication
ECPA	Electronic Communications Privacy Act
EOPS	Electronic Surveillance Operations and Sharing Unit
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act of 1978
IDW	Investigative Data Warehouse
IIR	Intelligence Information Report
IOB	Intelligence Oversight Board
ITOS	International Terrorism Operations Section
JTTF	Joint Terrorism Task Force
NFIP	National Foreign Intelligence Program
NSI	National Security Investigation
NSL	National Security Letter
NSLB	National Security Law Branch
OGC	Office of the General Counsel
OIG	Office of the Inspector General
OIPR	Office of Intelligence Policy and Review
OLC	Office of Legal Counsel
RFPA	Right to Financial Privacy Act
SAC	Special Agent in Charge
SSA	Supervisory Special Agent
TFOS	Terrorist Financing Operations Section
USAO	United States Attorneys' Offices

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.

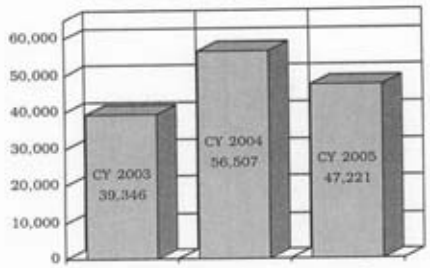
---

[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

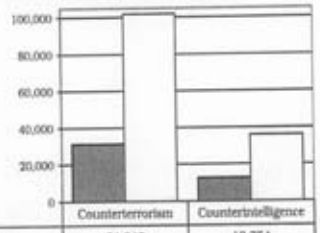
The number of NSL requests we identified significantly exceeds the number reported in the Department's first public annual report on NSL usage, issued in April 2006, because the Department was not required to include all NSL requests in that report. The Department's public report stated that in CY 2005 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]

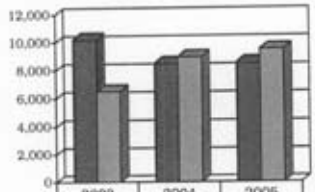
---

[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."

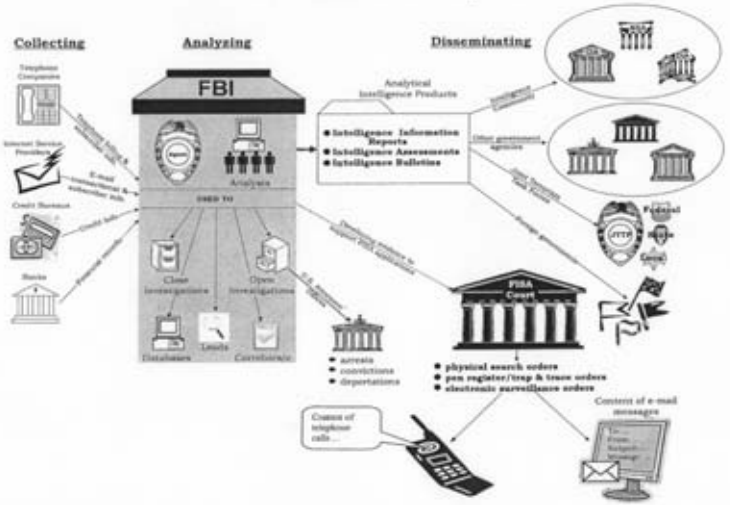
FBI personnel reported that the principal objectives for using NSLs are to:

- 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 intelligeuce 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, coutain 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 uot 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.

CHAPTER ONE
INTRODUCTION

In the Patriot Reauthorization Act, enacted in 2006, 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."[1] The Act required the OIG to conduct reviews of the use of national security letters for two separate time periods.[2] This report describes the results of the first OIG review of the FBI's use of national security letters (NSLs), covering calendar years (CY) 2003 through 2005.[3]

I. Provisions of the USA Patriot Act and Reauthorization Act

In October 2001, in the wake of the September 11 terrorist attacks, Congress passed the USA PATRIOT Act.[4] Section 505 of the Patriot Act expanded four existing statutes (the "national security letter statutes") that authorized the Federal Bureau of Investigation (FBI) to use national security letters to obtain certain specified types of information from third parties for use in authorized counterintelligence, counterterrorism, and foreign computer intrusion cyber investigations. As part of the Patriot Act legislation, Congress enacted a fifth NSL authority permitting the FBI to use national security letters to obtain consumer full credit reports in international terrorism investigations.

National security letters, which are written directives to provide information, are issued by the FBI directly to third parties, such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies, without judicial review. In these letters, the FBI

---

[1] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 119(a), 120 Stat. 192 (2006) (Patriot Reauthorization Act).

[2] Although the Act only required the OIG to include calendar years 2003 through 2004 in the first report, we elected to also include 2005 in this first report. The second report, which is due to Congress on December 31, 2007, will cover calendar year 2006.

[3] The Patriot Reauthorization Act also directed the OIG to conduct reviews on the use and effectiveness of Section 215 orders for business records, another investigative authority that was expanded by the Patriot Act. 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.

[4] The term "USA PATRIOT Act" is an acronym for the law entitled 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). This law is commonly referred to as "the Patriot Act."

can direct third parties to provide customer account information and transactional records, such as telephone toll billing records.[5]

The national security letter authorities expanded by the Patriot Act were originally scheduled to sunset on December 31, 2005, but were temporarily extended by Congress until it finalized a reauthorization bill. Congress passed the reauthorization bill in early 2006, and on March 9, 2006, the President signed into law the Patriot Reauthorization Act, which, among other things, reauthorized the five national security letter authorities.

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 –

(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;

---

[5] The statutes do not authorize the FBI to collect the content of telephone calls and e-mail. For that information, the FBI must obtain court approval or voluntary production of the records pursuant to 18 U.S.C. § 2702(b)(8) (2000).

(D) whether, and how often, the Department of Justice provided such information to law enforcement authorities for use in criminal proceedings; . . . .[6]

According to the Patriot Reauthorization Act, the OIG's first report on the FBI's use of national security letters is due to Congress on March 9, 2007.

I. Methodology of the OIG Review

In this review, the OIG conducted interviews of over 100 FBI employees, including personnel at FBI Headquarters in the Office of the General Counsel (FBI-OGC), Counterterrorism Division, and Counterintelligence Division, and personnel in four field divisions. We also interviewed officials in the Department's Criminal Division and National Anti-Terrorism Advisory Council Coordinators. We also attended background briefings regarding national security letters and the databases in which information derived from national security letters is stored and analyzed. We examined over 31,000 FBI documents from FBI Headquarters operational and support divisions and four field divisions pertaining to national security letters. Among the documents we analyzed were Headquarters guidance memoranda; correspondence; and reports by the FBI's Inspection Division, FBI-OGC, and Office of Professional Responsibility. In addition, we analyzed documents from the Department's Office of Legislative Affairs that included testimony, memoranda, and hearing transcripts regarding the oversight and reauthorization of the Patriot Act, including provisions affecting national security letter authorities and semiannual classified reports to Congress on the FBI's use of national security letter authorities.

OIG teams also examined FBI case files that contained national security letters and conducted interviews at four FBI field divisions in May and June 2006: Chicago, New York, Philadelphia, and San Francisco. These field divisions were selected from among the eight field divisions that issued the most national security letter requests during the period of our review, from 2003 through 2005. At the four field divisions, we conducted interviews of 52 FBI personnel, including an Assistant Director in Charge, Special Agents in Charge, Acting Special Agents in Charge, Assistant Special Agents in Charge, supervisory special agents overseeing counterterrorism and counterintelligence squads, Chief Division Counsel and Assistant Division Counsel, special agents, intelligence analysts, and intelligence research specialists.

---

[6] Patriot Reauthorization Act, § 119(b).

Also at the four field divisions, we examined a judgmental sample of 77 counterterrorism and counterintelligence investigative case files. Those files contained approximately 800 requests for information under four of the five national security letter authorities. Of that total, we reviewed up to 5 national security letters in each investigative file, for a total of 293 national security letters issued from January 1, 2003, through December 31, 2005. We reviewed those documents to determine whether the national security letters were issued in accordance with the relevant statutes, Attorney General Guidelines, and FBI policies. With regard to these national security letters, we reviewed documentation pertaining to case initiations, authorizations, delivery to the designated recipients, the recipients' production of documents and electronic media in response to the letters, retention of that information, and the analysis and dissemination of the information within the Department, to the intelligence community, and to others.

The OIG also analyzed the FBI-OGC's National Security Letter Database (OGC database), which the FBI uses for collecting information necessary to compile the Department's semiannual classified reports to Congress on NSL usage and, since passage of the Patriot Reauthorization Act, to compile the Department's annual public report on NSL usage. During the period of our review, the Department was directed to file semiannual classified reports to Congress reflecting the number of "NSL requests" the FBI made pursuant to three of the five national security letter authorities (see Chart 1.1). We also analyzed this OGC database to assess the accuracy and reliability of

CHART 1.1
Relationship Between NSLs and NSL Requests
(2003 through 2005)

In this report, we often refer to the number of national security letter requests rather than 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 numbers of requests made, not the number of letters issued. In this report, we follow that same approach. This chart shows the relationship we found between the number of investigations, NSLs, and NSL requests from 2003 through 2005 by counterterrorism and counterintelligence cases. Fewer than one percent of all NSL requests during this period were issued in foreign computer intrusion cyber investigations.

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

Source: FBI-OGC Database
*The NSL request totals on this chart are less than the [redacted] NSL requests noted above because they do not include NSL requests issued in connection with cyber investigations or the total number of NSL requests that were lost due to a malfunction of the OGC database.

the FBI's reports. We compared the OGC database entries to the documentation of the use of these authorities in the field divisions' investigative case files and performed other tests. These tests revealed significant errors in the OGC database, which we describe in Chapter Four. However, although we recognize the limitations of the OGC database, we used data from the OGC database for some of our analysis because it is the only source of centralized data on the FBI's use of NSLs.

During this review, we also distributed an e-mail questionnaire to the counterintelligence and counterterrorism squads in the FBI's 56 domestic field offices to attempt to determine the types of analytical products the FBI developed based on national security letters; the manner in which national security letter-derived information was disseminated within the Department, to other members of the intelligence community, and to others; and the occasions when such information was provided to law enforcement authorities for use in criminal proceedings.

II. Organization of the Report

This report is divided into eight chapters. Following this introduction, Chapter Two provides background on the use of national security letters, the Attorney General Guidelines which govern the FBI's conduct of national security investigations, and the roles of several FBI Headquarters divisions and components involved in the approval and operational use of national security letters.

Chapter Three describes the manner in which the FBI collects information by issuing national security letters and how it retains the information in investigative case files, shared computer drives, and databases.

Chapter Four presents data on the FBI's use of national security letters from 2003 through 2005. This information is based on data derived from the OGC database, the Department's semiannual classified reports to Congress on NSL usage, and our field work.

Chapter Five addresses other issues the Patriot Reauthorization Act directed the OIG to review regarding 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.

Chapter Six reports 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.

Chapter Seven reports other noteworthy facts or circumstances identified in the review, including the interpretation of the Attorney General Guidelines' requirement to use the "least intrusive collection techniques

feasible" with regard to the use of national security letters; uncertainty about the types of telephone toll billing records the FBI may obtain pursuant to an Electronic Communications Privacy Act (ECPA) national security letter; the review by Division Counsel of NSL requests; the issuance of NSLs from control files rather than investigative files, in violation of FBI policy; the FBI's use of "certificate letters" rather than Right to Financial Privacy Act (RFPA) national security letters to obtain records from Federal Reserve Banks; and the FBI's failure to include in the OGC database information reflecting the use of NSLs to obtain information on individuals who are not subjects of FBI investigations.

Chapter Eight contains a summary of our conclusions and our 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.

CHAPTER TWO
BACKGROUND

In this chapter we describe the five national security letter authorities and the Attorney General Guidelines that govern their use. We also describe the roles of FBI Headquarters divisions and field components in issuing and using these letters in national security investigations.

I. Background on National Security Letters

Over the last 20 years, Congress has enacted a series of laws authorizing the FBI to obtain certain types of information from third parties in terrorism, espionage, and classified information leak investigations without obtaining warrants from the Foreign Intelligence Surveillance Court or approval from another court.[7] These include five statutory provisions that authorize the FBI to obtain customer and consumer transactional information from communications providers, financial institutions, and consumer credit agencies by issuing national security letters (NSLs).[8] All but one of these provisions – the statute allowing access to consumer full credit reports in international terrorism investigations – predated the October 2001 passage of the Patriot Act. The authorizing statutes in effect prior to the Patriot Act required certification by a senior FBI Headquarters official that the FBI had "specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign

---

[7] FBI investigations of terrorism and espionage are called "national security investigations," which are conducted pursuant to the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003)(NSI Guidelines). NSLs are not authorized in connection with FBI conduct of ordinary criminal investigations or domestic terrorism investigations.

[8] The five statutes are:

1) 18 U.S.C. § 2709 (covering subscriber information and telephone toll billing records information and electronic communication transactional records);

2) 12 U.S.C. § 3414 (covering financial records);

3) 15 U.S.C. § 1681u (covering the names and addresses of all financial institutions at which a consumer maintains or has maintained an account; and the consumer's name, address, former addresses, places of employment or former places of employment);

4) 15 U.S.C. § 1681v (covering consumer reports and all other information in a consumer's file in international terrorism investigations); and

5) 50 U.S.C. § 436 (covering financial records, other financial information, and consumer reports in law enforcement investigations, counterintelligence inquiries, or security determinations). See Appendix A of this report for the text of the five statutes prior to the effective date of the Patriot Reauthorization Act.

The phrase "national security letter" was not used in any of the authorizing statutes, but was commonly used to refer to these authorities. The term was first used in legislation in the Patriot Reauthorization Act.

power or agent of a foreign power" as defined in the Foreign Intelligence Surveillance Act of 1978.[9]

A. The Patriot Act

The September 11 attacks prompted a reevaluation of the law enforcement and intelligence tools that were available to detect and prevent terrorist attacks. Among the topics Congress and the Department of Justice considered was the use of national security letters.[10] The Department reported in Congressional testimony that "in many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from Headquarters, and served."[11]

The Patriot Act significantly expanded the FBI's preexisting authority to obtain information through national security letters. 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 and substituting the lower threshold that the information requested be relevant to or sought for 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";
- Permitting, as a consequence of this lower threshold, national security letters to request information from communication providers, financial institutions, and consumer credit agencies

---

[9] See, e.g., 18 U.S.C. § 2709 (2000) ; 50 U.S.C. §§ 1801-1811 (2000).

[10] S. 1448, The Intelligence to Prevent Terrorism Act of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearing Before the Senate Select Comm. On Intelligence, 107th Cong. (2002); Dismantling the Financial Infrastructure of Global Terrorism: Hearing Before the House Comm. on Fin. Servs., 107th Cong. (2002); The Role of Technology in Preventing the Entry of Terrorists into the United States: Hearing Before the Senate Subcomm. on Tech., Terrorism, Gov't Info. of the Comm. on the Judiciary, 107th Cong. (2002).

[11] Hearing Before the House Comm. on the Judiciary, 107th Cong. 57-58 (2001) (Administration's Draft Anti-Terrorism Act of 2001). This view also was reflected in post-Patriot Act testimony at hearings considering whether to reauthorize the NSL authorities in the Patriot Act. See Tools Against Terror: How the Administration is Implementing New Laws in the Fight to Protect Our Homeland: Hearing Before the Subcomm. on Technology, Terrorism, and Gov't Info. of the Senate Comm. on the Judiciary, 107th Cong. 139 (2002) (statement of Dennis Lormel, Chief, Terrorist Financing Operations Section, Counterterrorism Division, FBI)("Delays in obtaining NSLs has long been identified as a significant problem relative to the conduct of counterintelligence and counterterrorism investigations.")

about persons other than the subjects of FBI national security investigations so long as the requested information is relevant to an authorized investigation; and

- Permitting Special Agents in Charge of the FBI's 56 field offices to sign national security letters, thus significantly expanding approval authority beyond senior FBI Headquarters officials.[12]

In addition to expanding preexisting NSL authorities, the Patriot Act added a new NSL authority permitting the FBI and certain other federal government agencies to use NSLs to obtain access to consumer full credit reports in international terrorism investigations pursuant to an amendment to the Fair Credit Reporting Act (FCRA).[13] Prior to this amendment, the FBI could use FCRA NSLs only to obtain basic financial institution and consumer-identifying information about the person's bank accounts, places of employment, and addresses.[14]

The Patriot Act did not alter existing provisions in the statutes barring recipients of national security letters from disclosing their receipt of the letters and from disclosing the records provided. These so-called "gag order" provisions prohibited NSL recipients from challenging NSLs in court. Similarly, NSL authorities prior to the Patriot Act did not provide an express mechanism by which the FBI could enforce an NSL in court if a recipient refused to comply. The Patriot Act also did not include any express enforcement mechanism.

The pre-Patriot Act statutes required the FBI to provide classified semiannual reports to Congress disclosing summary information about national security letter usage.[15] The Patriot Act continued to require classified reports to Congress on the FBI's use of its NSL authorities.

---

[12] Prior to the Patriot Act, approximately 10 FBI Headquarters officials were authorized to sign national security letters, including the Director, Deputy Director, and the Assistant Directors and Deputy Assistant Directors of the Counterterrorism and Counterintelligence Divisions. Under the Patriot Act, the heads of the FBI's 56 field offices (Assistant Directors in Charge or Special Agents in Charge) may also issue NSLs. Since enactment of the Patriot Act, approval to sign NSLs has also been delegated to the Deputy Director, Executive Assistant Director (EAD), and Assistant EAD for the National Security Branch; Assistant Directors and all Deputy Assistant Directors for the Counterterrorism, Counterintelligence, and Cyber Divisions; all Special Agents in Charge of the New York, Washington, D.C., and Los Angeles field offices, which are headed by Assistant Directors in Charge; the General Counsel; and the Deputy General Counsel for the National Security Law Branch in the Office of the General Counsel.

[13] 15 U.S.C. § 1681v (Supp. IV 2005).

[14] 15 U.S.C. § 1681u (2000).

[15] The national security letter authority in the National Security Act, which allows collection of financial records and information, consumer reports, and travel records, did not require reports to Congress. See 50 U.S.C. § 436 (2000).

B. Types of Information Obtained by National Security Letters

The type of information the FBI can obtain through national security letters includes:

Telephone and e-mail Information

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

Financial Information

- Financial information such as 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.

Consumer Credit Information

- Names and addresses of all financial institutions at which a consumer maintains or has maintained an account;
- Identifying information respecting a consumer . . . limited to name, address, former addresses, places of employment, or former places of employment; and
- Consumer reports of a consumer and all other information in a consumer's file (full credit reports).

C. The Patriot Reauthorization Act

The Patriot Reauthorization Act reauthorized all of the provisions that were subject to lapse or "sunset" in the original Patriot Act (with some modification), including the five NSL authorities.[16] One of the modifications

---

[16] Pub. L. No. 109-177, § 102(a) (2006). The Patriot Reauthorization Act modified the non-disclosure requirements regarding national security letters. An NSL recipient may now disclose the NSL in connection with seeking legal advice or complying with the NSL. In

required the Department to issue, in addition to its semiannual classified reports, annual public reports that disclose certain data on the FBI's national security letter requests. The public report must include the aggregate number of NSL requests issued pursuant to the five NSL statutes including, for the first time, data on the use of the full credit report authority established pursuant to the Fair Credit Reporting Act, the only new NSL authority enacted by the Patriot Act.

The Department's first public annual report pursuant to the Patriot Reauthorization Act on the use of NSL authorities was issued on April 28, 2006.[17] The report stated that during calendar year 2005, federal government agencies issued 9,254 "NSL requests" involving 3,501 different "United States persons."[18]

II. The Four National Security Letter Statutes

The following is a brief overview of the four statutes authorizing the FBI to issue five types of national security letters.

A. 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."[19] The RFPA requires federal government agencies to provide individuals with advance notice of requested disclosures of personal financial information and gives individuals an opportunity to challenge the request before disclosure is made to law enforcement authorities.[20]

The first NSL statute was passed in 1986 as an amendment to the RFPA. It created an exception to the advance notice requirement by permitting the FBI to obtain financial institution records in foreign

---

(cont'd.)

addition, the Patriot Reauthorization Act permits the NSL recipient to challenge compliance with the NSL and the non-disclosure requirement in federal court. In addition, the government may seek judicial enforcement of NSLs in the event of non-compliance.

[17] See Letter from William E. Moschella, Assistant Attorney General, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (April 28, 2006), at 3.

[18] Id. In Chapter Four we describe the categories of NSL requests that are included and excluded from the public report.

[19] H.R. Rep. No. 95-1383, at 33 (1978), reprinted in 1978 U.S.C.C.A.N. 9273, 9305. The RFPA was enacted in response to the Supreme Court's decision in United States v. Miller, 425 U.S. 435 (1976), which held that customers of banking services had no expectation of privacy under the Fourth Amendment and therefore could not contest government access to their records.

[20] 12 U.S.C. §§ 3401-3422 (2000).

counterintelligence cases. Before the Patriot Act, the FBI could issue RFPA NSLs upon certification of

> specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power. . . .[21]

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.[22]

In December 2003, Congress amended the RFPA to expand the definition of "financial institutions" to which NSLs could be issued, including entities such as rental car companies, automobile dealerships, credit unions, issuers of travelers' checks, pawnbrokers, and real estate companies.[23]

The FBI can disseminate information derived from the RFPA national security letters only in accordance with the Attorney General Guidelines governing national security investigations and can disseminate such information to other federal agencies only if the information is clearly relevant to the authorized responsibilities of those federal agencies.[24]

B. The Electronic Communications Privacy Act

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA), which extended statutory protection to electronic and wire communications stored by third parties such as telephone companies and Internet Service Providers.[25] The statute restricted the government's access to live telephone transactional data, such as the telephone numbers that a particular telephone number calls or received (known as "pen register" and

---

[21] 12 U.S.C. § 3414(a)(5)(A) (2000).

[22] 12 U.S.C. § 3414(a)(5)(A) (2000 & Supp. IV 2005). Financial records accessible to the FBI under the RFPA were also subject to compulsory process through subpoenas, search warrants, and formal requests, all of which, with limited exceptions, required notice to the customer.

[23] See 12 U.S.C. § 3414(d) (2000 & Supp. IV 2005), as amended by the Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-77, § 374(a) (2004), which incorporated the definition of "financial institution" set forth in 31 U.S.C. §§ 5312(a)(2) and (c)(1).

[24] 12 U.S.C. § 3414(a)(5)(B) (2000).

[25] 18 U.S.C. § 2709 (1988).

"trap and trace" data). The ECPA required the government to obtain a court order for which it must certify the relevance of the information to an ongoing criminal investigation.[26] The statute requires that subjects of government requests for these records be given advance notice of the requested disclosure and an opportunity to challenge the request.

However, the ECPA allowed 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. Before the Patriot Act, the FBI could obtain ECPA NSLs upon certification of

> specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power. . . .[27]

Since the Patriot Act, the FBI must certify 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.[28]

In 1993, Congress expanded the ECPA NSL authority by permitting access to the subscriber and toll billing records of additional persons, such as those who were in contact with agents of a foreign power.[29] Congress amended the ECPA again in 1996 by defining "toll billing records" to expressly include "local and long distance toll billing records."[30]

Recipients of ECPA NSLs were prohibited until the Patriot Reauthorization Act from disclosing to any person that the FBI had sought or obtained the requested information.[31]

---

[26] A "pen register" is a device that records the numbers that a target telephone is dialing. A "trap and trace" device captures the telephone numbers that dial a target telephone. See 18 U.S.C. § 3127 (2000).

[27] 18 U.S.C. § 2709(b)(1)(B) (2000).

[28] 18 U.S.C. § 2709(b)(2) (2000 & Supp. IV 2005).

[29] Pub. L. No. 103-142, § 2, 107 Stat. 1491 (1993). The 1993 amendment also provided additional congressional reporting requirements. Id.

[30] Intelligence Authorization Act for Fiscal Year 1997, Pub. L. No. 104-293, § 601(a), 110 Stat. 3461 (1996).

[31] 18 U.S.C. § 2709(c) (2000).

The FBI may disseminate information obtained from ECPA NSLs to other federal agencies "only if such information is clearly relevant to the authorized responsibilities of such agency."[32]

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.[33]

C. The Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA), as amended by the Patriot Act, authorizes two types of national security letters, FCRAu and FCRAv NSLs. The FCRA was enacted in 1970 to protect personal information collected by credit reporting agencies.[34] The FCRA prohibits the disclosure of information collected for the purpose of establishing eligibility for credit, insurance, employment, and other related purposes.

However, Congress amended the FCRA in 1996 to authorize the FBI (and certain other government agencies) to issue national security letters 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 pursuant, referred to as FCRAu NSLs; and consumer identifying information limited to name, address, former addresses, places of employment and former places of employment.[35] Before the Patriot Act, the FBI could obtain FCRA NSLs upon certification that

> (1) such information is necessary for the conduct of an authorized foreign counterintelligence investigation; and
>
> (2) there are specific and articulable facts giving reason to believe that the consumer –
>
> (A) is a foreign power or a person who is not a United States person and is an official of a foreign power; or
>
> (B) is an agent of a foreign power and is engaging or has engaged in an act of international terrorism or clandestine

---

[32] 18 U.S.C. § 2709(d) (2000).

[33] 18 U.S.C. § 2709(a) (2000). ECPA requires a warrant for the interception and surveillance of the content of a telephone call or e-mail communication. See 18 U.S.C. §§ 2511 (Wiretap Act) and 3121 (Pen Register Act). See also 18 U.S.C. § 2702(b)(8) (2000).

[34] 15 U.S.C. § 1681 et seq (2000).

[35] 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).

> intelligence activities that involve or may involve a violation of criminal statutes of the United States.[36]

Since the Patriot Act, the FBI must certify that the information 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.[37]

In 2001, the Patriot Act amended the FCRA to add a new national security letter authority (FCRAv). The Patriot Act amendment to the FCRA authorizes the FBI and other government agencies that investigate or analyze international terrorism to obtain a consumer reporting agency's credit reports and "all other" consumer information in its files in accordance with the following provision:

> [A] consumer credit agency shall furnish a consumer credit report of a consumer and all other information in a consumer's files to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.[38]

This NSL authority is available to the FBI only in connection with international terrorism investigations. Until the Patriot Reauthorization Act, recipients of FCRA NSLs were prohibited from disclosing to any person that the FBI had sought or obtained the requested information.

D. The National Security Act

In 1994, in the wake of the espionage investigation of former Central Intelligence Agency employee Aldrich Ames, Congress enacted an additional NSL authority by amending the National Security Act of 1947. The amendment authorized NSLs to be issued in connection with investigations of improper disclosure of classified information by government employees.[39]

---

[36] 15 U.S.C. § 1681u (2000).

[37] 15 U.S.C. § 1681u(a)-(b) (2000 & Supp. IV 2005).

[38] Patriot Act, § 358(g) (2001). Unlike other NSL statutes, the full credit report NSL authority is available not only to the FBI but also to other federal government agencies. This provision does not contain an express prohibition on dissemination.

[39] 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.

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."[40] Prior to the Patriot Reauthorization Act, recipients of National Security Act NSLs, like recipients of RFPA and ECPA NSLs, were prohibited from disclosing to any person that the FBI had sought or obtained the requested information, with some exceptions.

National Security Act NSLs are rarely used by the FBI.[41]

III. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection

National security letters may be issued by the FBI in connection with national security investigations, which are governed by Attorney General Guidelines.

During the time period covered by this report, 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 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).[42]

A. Levels of Investigative Activity under the FCI Guidelines (January 1, 2003 – October 31, 2003)

The FCI Guidelines authorized two levels of investigative activity: preliminary inquiries and full investigations. The FCI Guidelines identified the basis or "predicate" for opening each type of investigation as well as the authorized techniques permitted at each stage. Full foreign counterintelligence investigations permitted the FBI to gather information and conduct activities

> to protect against espionage and other intelligence activities, sabotage, or assassinations conducted by, for or on behalf of

---

[40] 50 U.S.C. § 436(a)(1) (2000).

[41] These NSLs were used to obtain bank account, credit card, and loan transaction information to support the predicate for the FBI's espionage investigation of Aldrich Ames. See Commission for Review of FBI Security Programs (March 31, 2002)(Webster Commission), at 66.

[42] Both sets of Guidelines are partially classified.

> foreign powers, organizations or persons, or international terrorist activities . . . .[43]

The FCI Guidelines did not permit the FBI to use national security letters during preliminary inquiries, only during full investigations. However, following the September 11 attacks, the Attorney General authorized the use of NSLs during preliminary inquiries with prior approval by the Attorney General and the FBI Director.[44]

B. Levels of Investigative Activity under the NSI Guidelines (October 31, 2003)

The NSI Guidelines issued on October 31, 2003, which remain in effect today, 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 – and prescribe the investigative techniques available during each investigative stage.

Threat Assessments: Under the NSI Guidelines, the FBI is authorized to conduct threat assessments

[redacted].[45]

The NSI Guidelines do not permit the FBI to issue national security letters during a threat assessment.

Preliminary Investigations: Under the NSI Guidelines, a preliminary investigation (previously known as a "preliminary inquiry") can be initiated or "opened" by certain Headquarters officials or by a field office with the approval of certain field supervisors. A preliminary investigation can be opened when there is information or an allegation indicating the existence of one of several identified circumstances. In preliminary investigations, FBI

---

[43] FCI Guidelines, § II(D).

[44] In January 2003, the Attorney General issued a memorandum modifying the FCI Guidelines by authorizing designated Headquarters officials and Special Agents in Charge designated by the FBI Director to issue ECPA, RFPA, and FCRAu NSLs during preliminary inquiries.

[45] NSI Guidelines, § II(A). The authorized techniques permitted during threat assessments are classified.

agents are authorized to employ the activities and techniques permitted to be used during threat assessments as well as certain other investigative techniques, including the issuance of national security letters.[46]

Full Investigations: Under the NSI Guidelines, full investigations may be opened when there are "specific and articulable facts giving reason to believe that a threat to the national security may exist."[47] During these investigations, FBI agents are authorized to employ the activities and techniques permitted to be used during threat assessments and preliminary investigations, as well as certain other investigative techniques.[48] National security letters are permitted to be used during full investigations.

The NSI Guidelines also provide guidance concerning the selection of authorized techniques during different investigative stages:

> Choice of Methods. The conduct of investigations authorized by these Guidelines may present choices between the use of information collection methods that are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. As Executive Order 12333 § 2.4 provides, "the least intrusive collection techniques feasible" are to be used in such situations. It is recognized, however, that the choice of techniques is a matter of judgment. The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a threat to the national security or the strength of the information indicating its existence. This point is to be particularly observed in investigations relating to terrorism.[49]

IV. The Role of FBI Headquarters and Field Offices in Issuing and Using National Security Letters

We describe below the responsibilities of Headquarters and field divisions assigned to conduct or support the FBI's investigative and intelligence activities in national security investigations.

A. FBI Headquarters

During most of the period of this review, three FBI Headquarters divisions were responsible for supervising the FBI's counterterrorism,

---

[46] The additional techniques permitted during preliminary investigations are classified.

[47] NSI Guidelines, Introduction, A.

[48] The additional techniques permitted during full investigations are classified.

[49] NSI Guidelines, § I(B)(2).

counterintelligence, and cyber programs: the Counterterrorism Division, Counterintelligence Division, and Cyber Division. These programs were implemented through the counterterrorism, counterintelligence, and cyber squads in the FBI's 56 domestic field divisions and through the establishment of operational support sections within the Headquarters divisions.

1. Counterterrorism Division

The division's mission is to identify and disrupt potential terrorist plots, freeze terrorist finances, share information with law enforcement and intelligence partners world-wide, and provide strategic and operational threat analysis to the intelligence community. Agents assigned to counterterrorism squads use information derived from national security letters to analyze non-content telephone and Internet communications, financial records, financial institution and consumer-identifying information, and consumer full credit reports.

2. Counterintelligence Division

The division's mission involves counterproliferation, counterespionage, and protection of critical national assets. Agents assigned to counterintelligence squads use information obtained from national security letters to analyze non-content telephone and Internet communications, financial records, and financial institution and consumer-identifying information.

3. Cyber Division

The division's mission is to protect the United States against cyber-based attacks and high technology crimes. Its agents provide support for computer-related counterterrorism and counterintelligence investigations with an international nexus, including foreign computer intrusion cyber investigations.

4. Directorate of Intelligence

The directorate's mission is to meet current and emerging national security and criminal threats by assuring that the FBI proactively targets threats to the United States; providing useful, appropriate, and timely information and analysis; and building and sustaining FBI-wide intelligence policies and capabilities. The directorate has no officials who are authorized to sign national security letters. However, during the period covered by our review the field-based Field Intelligence Groups, which report to this directorate, performed significant analytical work on data derived from national security letters in support of the FBI's counterterrorism, counterintelligence, and cyber programs. The directorate also serves as the FBI's primary liaison for dissemination and receipt of intelligence

information outside the FBI and has the final review authority over intelligence products to be disseminated outside the FBI, including information derived from national security letters.

5. Office of the General Counsel (FBI-OGC)

The National Security Law Branch (NSLB) of FBI-OGC provides legal advice, guidance, and training on the FBI's use of national security letter authorities; collects data on NSL usage from Headquarters and field divisions for purposes of preparing the Department's required reports to Congress; prepares NSLs for the signatures of the General Counsel, the Deputy General Counsel for NSLB, and certain Headquarters officials; provides technical support regarding retention and dissemination of NSL-derived information; identifies, evaluates, and corrects misnse of NSL authorities; evaluates possible Intelligence Oversight Board (IOB) violations reported by field and Headquarters personnel and reports some of these matters to the President's Foreign Intelligence Oversight Board; and develops legislative proposals and responds to congressional requests for information about the FBI's use of its NSL authorities.

B. FBI Field Divisions

The FBI's 56 field divisions have counterterrorism, counterintelligence, and cyber squads that investigate cases related to national security threats or potential threats. Field supervisors are authorized to initiate counterterrorism, counterintelligence, and cyber investigations, and Special Agents in Charge are authorized to sign national security letters. Additional FBI and non-FBI field personnel who are responsible for reviewing and analyzing information obtained through national security letters are:

1. Chief Division Counsel

Chief Division Counsel (CDCs) in all 56 FBI field divisions report to the Special Agents in Charge of the field division and are responsible for reviewing all national security letters prepared for the signature of the Special Agent in Charge. CDCs in large field divisions sometime delegate this authority to Assistant Division Counsel. The responsible Chief Division Counsel or Assistant Division Counsel examines approval documents and the draft national security letters for legal sufficiency, corrects errors, seeks additional information when needed, and forwards the approval package to the Special Agent in Charge. CDCs also provide training to agents serving on counterterrorism, counterintelligence, and cyber squads, provide advice on how to address legal issues arising from the use of NSL authorities, and assist case agents in reporting possible IOB violations arising from the use of these authorities to FBI-OGC.

2. Field Intelligence Groups

Field Intelligence Groups (FIG) were established in all 56 field divisions by October 2003. They include special agents, intelligence analysts, language analysts, and special surveillance groups. FIG personnel conduct intelligence analyses, direct the collection of information to fill intelligence gaps, and are responsible for disseminating intelligence products to internal and external customers, including state and local law enforcement. FIG personnel analyze information derived from national security letters, often relating it to other cases within the field division and other field divisions. The intelligence directorate's Field Oversight Unit develops, supports, and provides oversight of the FIGs, which are managed in each field division by an Assistant Special Agent in Charge.

CHAPTER THREE
THE FBI'S COLLECTION AND RETENTION OF INFORMATION OBTAINED FROM NATIONAL SECURITY LETTERS

In this chapter we describe the process by which FBI agents obtain approval to issue national security letters. We also describe the manner in which the FBI obtains information through national security letters from third parties and retains such information in FBI Headquarters and field divisions.

I. The FBI's Process for Collecting Information Through National Security Letters

According to our interviews of FBI personnel, case agents conducting counterintelligence, counterterrorism, or foreign computer intrusion cyber investigations who need telephone or e-mail transactional activity, subscriber information, financial transactions, or credit information relevant to their investigations first assess the most effective investigative technique available at a particular stage of the investigation. For example, if the facts developed indicate a nexus to possible criminal activity, agents can ask the United States Attorney's Office to open a grand jury investigation, which allows prosecutors to issue federal grand jury subpoenas to obtain third party records.[50] If there is a criminal nexus, prosecutors often prefer to use grand jury subpoenas because they generally can obtain grand jury subpoenas quickly and recipients respond more promptly to grand jury subpoenas than they do to NSLs. However, issuance of a grand jury subpoena risks public disclosure that the government is conducting a national security investigation. As a result, agents often consider alternative investigative techniques, such as national security letters, which avoid public disclosure of the existence of an investigation.

To obtain approval within the FBI to issue national security letters, FBI agents must determine that information available pursuant to one of the national security letter authorities is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities and, with respect to an investigation involving a "U.S. person," is "not solely conducted on the basis of activities protected by the First Amendment."[51] Case agents assigned to counterterrorism, counterintelligence, or cyber squads are responsible for preparing the

---

[50] Terrorism investigations often have a potential criminal nexus under statutes proscribing material support of terrorism and conspiracy, and federal statutes criminalizing threats against public facilities, aircraft, and other transportation systems, as well as possession of weapons of mass destruction.

[51] 18 U.S.C. §§ 2709(b)(1) and 2709(b)(2); 12 U.S.C. § 3414 (a)(5)(A); 15 U.S.C. § 1681u(a); 15 U.S.C. § 1681v(a).

documentation necessary to secure approval to issue a national security letter. Case agents are encouraged to check FBI databases, such as the Automated Case Support (ACS) system and Telephone Applications, a specialized application storing telephone record data, to determine whether the information they need has previously been obtained by the FBI or is available through public search engines or commercial databases.

FBI administrative policy, set forth in the partially classified National Foreign Intelligence Program (NFIP) Manual and on NSLB's Intranet website, requires that case agents prepare two documents to obtain an NSL: (1) an electronic communication (EC) seeking supervisory approval for the national security letter and (2) the national security letter itself.

1. Electronic Communication (Approval EC)

The EC used to obtain approval of national security letters serves four functions. It:

- documents the predication for the national security letter by stating why the information was relevant to an authorized investigation;
- documents the approval of the national security letter by appropriate personnel;
- includes information needed to fulfill congressional reporting requirements; and
- transmits copies of the request to the FBI-OGC; FBI Headquarters Counterterrorism, Counterintelligence, or Cyber Division; and, when the recipient is not located in the field division issuing the national security letter, the field division that is asked to serve the national security letter.

During the period covered by our review, NSLB attorneys developed eight standard formats for the approval ECs that included routine elements common to all NSL requests, data elements needed for congressional reporting, and descriptions of the elements that were to be included in the national security letter package. NSLB modified the standard formats as national security letter statutes were revised and internal FBI administrative policy changed.

As discussed in Chapter Two, the Patriot Act lowered the predication standard for national security letters from "specific and articulable facts giving reasons to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power" to "relevan[ce] to an authorized investigation to protect against international terrorism or clandestine intelligence activities." The standard form used during the period covered by this review required that case agents provide

justification for opening or maintaining the investigation and "briefly state the relevance of the requested records to the investigation."[52]

To enable the FBI to collect data for its semiannual congressional reporting requirements, the following information also is required to be included in the approval EC: (1) for RFPA financial record NSLs, ECPA toll billing and electronic communication transactional records NSLs, and FCRA NSLs, the investigative subject's status as a "U.S. person" or "non-U.S. person"; (2) the type of national security letter issued; and (3) a list of the individual telephone numbers, e-mail addresses, account numbers, or other records for which information is sought.[53]

For field division-initiated national security letters, the Supervisory Special Agent of the case agent's squad, the Chief Division Counsel, and the Assistant Special Agent in Charge are responsible for reviewing the approval EC and the national security letter prior to approval by the Special Agent in Charge. Division Counsel are required to review the national security letters 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) initials the approval EC and signs the national security letter.[54] For national security letters generated by Headquarters, there is a parallel requirement for generating the approval paperwork for the signature of specially designated Headquarters officials.[55] Accordingly, the approval EC includes an "approved by" section that reflects the names of the reviewing

---

[52] We discuss in Chapter Seven the circumstances that led to a February 2006 modification of models for NSL approval ECs, which now require a "full explanation of the justification for opening and maintaining the investigation of the subject" and to "fully state the relevance of the requested records to the investigation."

[53] For purposes of the reporting requirement, a "United States person" is defined as

> a citizen of the United States, an alien lawfully admitted for permanent residence . . ., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States . . . ."

50 U.S.C. § 1801(i). The congressional reporting requirements are described in Chapter Four.

[54] Certifying officials are not authorized to further delegate signature authority. Accordingly, Acting Special Agents in Charge are not authorized to sign national security letters.

[55] While NSLB encourages Headquarters operating divisions to utilize the NSLB Deputy General Counsel as the authorizing official, they are not required to do so. However, a legal review through NSLB is required.

and approving officials, who enter their initials on the hard copy of the document.

Field personnel in the four field offices we visited during the review told us that it takes from two to five days to obtain approval to issue NSLs. However, if there is no Special Agent in Charge in place in a field office, NSLs must be sent to another field office for approval by another Special Agent in Charge. Several Special Agents in Charge and Acting Special Agents in Charge told us that this has led to delays of as long as two weeks in securing approval to issue NSLs.

The approval EC also includes directions, known in FBI parlance as "leads," to other FBI offices for actions that these offices are directed to take regarding the national security letter. Leads are "set" electronically through the FBI's ACS computer system when the approval ECs are uploaded into the system. FBI personnel are responsible for checking ACS periodically to determine whether leads have been assigned to them. Leads also may be sent in hard copy via the FBI's interoffice mail delivery system. The initiating field office also includes a lead to NSLB that instructs it to record the appropriate information needed to fulfill congressional reporting requirements and an informational lead notifying the Counterterrorism, CounterIntelligence, or Cyber Division of the national security letter.

A case agent from the field office squad initiating the national security letter (the "office of origin") hand carries the letter to the designated recipient if it is located in the field division. If the NSL recipient is located in another field division, the office of origin sets a lead to the field office where the recipient is located with instructions to personally deliver the national security letter to the recipient.

2. The National Security Letter

A national security letter is the operative document that directs a third party to provide specific records. Although the internal documentation supporting the approval of national security letters is classified, neither the letters themselves nor the information provided to the FBI in response to the letters is classified.

As mentioned previously, during the period covered by our review NSLB developed and posted on its Intranet web site eight standard formats or models for the different types of national security letters that request the following categories of information, each of which was derived from one of the four statutory national security letter authorities in the Electronic Communications Privacy Act (items 1 - 4), the Right to Financial Privacy Act (item 5), or the Fair Credit Reporting Act (items 6, 7 and 8):

1. Telephone subscriber information;
2. Telephone toll billing records;
3. Electronic (e-mail) subscriber information;

4. Electronic communication transactional records;
5. Financial records;
6. Identity of financial institutions;
7. Consumer identifying information; and
8. Credit reports.

National security letters typically are addressed to an established point of contact at the entity possessing the records. For major national communication providers and other routine recipients of national security letters, NSLB posts a list of known points of contact on its Intranet website.

The first paragraph of the national security letter identifies the statutory authority for the request and the types of records requested. For example, a national security letter under the Fair Credit Reporting Act would reference 15 U.S.C. § 1681u(a) as the statutory authority and would request the names and addresses of all financial institutions at which a particular consumer maintains or has maintained an account. The letters also provide the identifying information for the specific individual (such as name, address, date of birth, or social security number), telephone number, or e-mail/Internet Protocol address, and specify a precise time period for which information is requested.

The national security letter also contains a statutorily required certification 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.

In conformity with the non-disclosure provisions in the NSL statutes, the next paragraph of the letter notifies the recipient that no officer, employee, or agent of the entity may disclose that the FBI sought or obtained the requested information or records. The last paragraph instructs the recipient to provide the records personally to an FBI representative at the field division that served the national security letter.

National security letters also may include an attachment that explains the specific types of records that the FBI is requesting or that the recipient may deem to be responsive. For example, attachments to the Electronic Communications Privacy Act and Right to Financial Privacy Act national security letters list the types of information that the recipient might consider to be "toll billing records information" or a "financial record."

The FBI's practices regarding the delivery methods and designated response times noted in the NSLs evolved during the period covered by our review. In response to delays encountered by the personal delivery requirement, NSLB concluded that FBI personnel could, with minimal risk,

use certain delivery services to deliver national security letters, such as the U.S. Postal Service or restricted delivery options offered by private delivery services.[56]

Some FBI agents complained to NSLB that failure to designate a due date or "return date" in the body of the NSL led to delayed responses by some recipients, which sometimes compromised time-sensitive investigations. NSLB concluded that there was no legal restriction against including a return date (much as a grand jury subpoena or administrative subpoena includes a specified "return date").

Headquarters and field personnel in the four field divisions we visited told us that there is no FBI policy or directive requiring the retention of signed copies of national security letters or any requirement to upload national security letters into ACS. We found that the FBI has no uniform system for tracking responses to national security letters, either manually or electronically.[57] Instead, individual case agents are responsible for following up with NSL recipients to ensure timely and complete responses. Case agents are also responsible for ensuring that the documents or electronic media provided to the FBI match the requests, both as to content and time period; analyzing the responses; and, depending upon the type of records, providing the documents or other materials to FBI intelligence or financial analysts who also analyze the information received.

II. The FBI's Retention of Information Obtained from National Security Letters

FBI case agents who obtain information from national security letters retain the information in different ways and in a variety of formats. The FBI has not issued general guidance regarding the retention of this information. The manner in which case agents retain the information depends upon the NSL type, the size and format of the response, and the manner in which the data is to be analyzed.

The case agents and squad supervisors we interviewed told us that they prefer to receive responses in electronic format for ease of storage and analysis. However, case agents and squad supervisors told us that the majority of the responses to all types of national security letters during the

---

[56] See EC from FBI-OGC to All Field Offices, *Legal Advice and Opinions: Service of National Security Letters* (June 29, 2005). The recipient could return responsive documents to the FBI via the same method. However, FBI personnel in the field offices we visited told us that the national security letters and responsive documents were usually personally delivered.

[57] In one field office we visited, the Special Agent in Charge maintains a control file with copies of signed national security letters, but this does not serve as a tracking system for responses.

period covered by our review were delivered in hard copies.[58] Field personnel told us that some major telephone companies provide telephone toll billing records and subscriber information in electronic format.

After inventorying the hard copy response to confirm that the information received matches the information requested in the NSL, the case agents generally prepare and upload an EC into ACS that documents receipt of the information. If the responsive records are relatively small in volume, the records are placed in the investigative case file or in a sub-file created to store information derived from NSLs. If the response to the NSL is voluminous, such as hundreds of pages of toll billing records or bank records, the documents are placed in centralized storage and the case agent completes a tracking form noting where the data is located.

If the response to the NSL is in an electronic format, such as a computer diskette, either the case agent or analyst initially reviews the response to confirm that the response matches the request and prepares the EC documenting receipt of the records. For example, the EC documenting receipt of ECPA telephone toll billing records or e-mail subscriber information states that the telephone number or e-mail address did or did not belong to the investigative subject or other target of the NSL. The case agent, data clerk, or analyst then provides the computer diskette or other electronic medium to an intelligence assistant or analyst, who is responsible for uploading the data into the pertinent database, such as the Telephone Applications database.[59]

Once an EC is uploaded into ACS documenting receipt of the response to an NSL, authorized users of ACS may access the EC's contents. During the period covered by our review, there were approximately 29,000 authorized accounts issued for FBI personnel permitting them to access ACS, and approximately 5,000 accounts issued for non-FBI personnel.[60] The vast majority of the non-FBI account holders were officers serving on task forces, such as the Joint Terrorism Task Forces, the Foreign Terrorist Tracking Task Force, and the National Joint Terrorism Task Force. The remaining accounts were provided to staff in organizations such as the

---

[58] FBI officials told us that some of the smaller communication providers and Internet service providers furnish NSL data in hard copy form. This placed a significant burden on FBI support personnel who sometimes were required to manually enter the data into a word processing program for uploading and analysis.

[59] Telephone Applications contains raw data derived from NSLs, known as "metadata," including the call duration. It does not store the contents of telephone conversations. During the period covered by our review, approximately 17,000 FBI personnel and approximately 2,000 non-FBI personnel had accounts permitting them to access the FBI's specialized application for telephone record data.

[60] Case agents may restrict FBI and non-FBI personnel from accessing certain electronic files in ACS and other databases in highly sensitive cases.

Department of Homeland Security, the Terrorist Screening Center, and the National Counterterrorism Center.

Raw data derived from national security letters or the analysis developed from the raw data are often used to create spreadsheets that are stored on the computer hard drives of Headquarters or field office personnel. As we discuss in Chapter Five, case agents and analysts told us that they generate these types of spreadsheets to establish communication and financial networks between investigative subjects and others. In addition, Headquarters and field offices have shared or "networked" computer drives that permit all case agents, analysts, and support personnel on a particular squad or a larger universe of users in the field office or Headquarters division to access them. In such cases, raw NSL data or the analytical products derived from this data are retained on these shared drives.

If a field or Headquarters supervisor determines that a more formal analytical intelligence product, such as an Intelligence Information Report or Intelligence Bulletin, should use information from NSLs and be shared with other members of the intelligence community or others, analysts on the field-based Field Intelligence Groups or the Headquarters Directorate of Intelligence prepare these products.[61] Electronic versions of these products are stored on field and Headquarters hard drives and, if a decision is made by the Directorate of Intelligence to disseminate them, are uploaded into the databases that are accessed by FBI and non-FBI personnel with authorized accounts.

We learned that the FBI's retention practices regarding information received in response to NSLs in excess of what was requested, whether due to FBI or third-party error, varies. If a field case agent determines that the NSL recipient provided more information than was requested, the case agent is responsible for notifying the Chief Division Counsel (CDC) and sequestering the information. However, we found that FBI-OGC did not issue guidance to all CDCs as to the mechanics of sequestering this information until November 2005. Instead, FBI-OGC provided ad hoc guidance to field agents or Division Counsel who contacted FBI Headquarters with questions.[62]

In our review, we learned of instances in which the excess records were destroyed, returned to the NSL recipient, or sequestered and given to

---

[61] In Chapter Five, we describe how information derived from national security letters is used in the development of these intelligence products.

[62] Eventually, in November 2006 NSLB sent guidance to the field that outlined the steps to be taken in these circumstances. The guidance memorandum stated that the agent should send the information to the CDC for sequestering, pending resolution of the matter. The memorandum also stated that NSLB would determine whether the sequestered information must be destroyed, returned to the provider, or may be used by the FBI, and whether the matter is reportable to the IOB.

the Chief Division Counsel. However, in other instances we found that case agents retained the information and sought approval to issue a new NSL to cover the excess information. Case agents and supervisors in the four field offices we visited told us that information provided in excess of what was requested in the NSL was not uploaded into ACS or other FBI databases.[63]

As noted above, the principal FBI databases that contain raw data derived from national security letters are ACS and a specialized application for telephone data. ACS is the FBI's centralized case management system. NSL data is periodically downloaded from ACS and Telephone Applications into the FBI's Investigative Data Warehouse (IDW), a centralized repository for intelligence and investigative data with advanced search capabilities.[64] Raw data derived from national security letters also is retained in various classified databases operated by the FBI and other members of the intelligence community.

---

[63] We identified one instance in which the FBI uploaded into the Telephone Applications database data the FBI had improperly acquired in response to an ECPA NSL. We describe this matter in Chapter Six.

[64] According to the FBI, the Investigative Data Warehouse contains data from approximately 50 different FBI and other government agency databases and holds over 560 million records. The FBI estimated in December 2006 that approximately 12,000 FBI and non-FBI personnel have user accounts to access IDW, approximately 30 percent of which were issued to non-FBI personnel, such as Task Force Officers on the Joint Terrorism Task Forces (JTTFs). *FBI Oversight:* Hearing Before the Senate Comm. on the Judiciary, 109th Cong. 6 (2006) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigations.

CHAPTER FOUR
NATIONAL SECURITY LETTER REQUESTS ISSUED BY THE FBI FROM 2003 THROUGH 2005

In this Chapter, we describe the FBI's use of national security letters during calendar years 2003 through 2005. In Section I, we discuss several problems with the FBI-OGC National Security Letter database (OGC database) that affect the accuracy of the information in this database. In Section II, while noting the limitations of the OGC database, we present data on the FBI's NSL usage that we developed from the Department's semiannual classified reports to Congress, the OGC database, and our examination of investigative files in four FBI field offices.

I. 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.[65] 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."[66] The data in the reports were drawn from the OGC database that was developed specifically to collect information for the Department's semiannual classified reports to Congress. The OGC database is the only centralized repository of data reflecting the FBI's use of national security letter authorities.

---

[65] The Department was required to report 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 (financial records, other financial information, and consumer reports) NSL statutes. In addition 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.

[66] 50 U.S.C. § 1801(i) defines a "United States Person" as:

> a citizen of the United States, an alien lawfully admitted for permanent residence . . ., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States . . . ."

However, as we describe below, several flaws with internal reporting by the FBI, as well as structural problems with the OGC database, affect the accuracy of the data and therefore the accuracy of the reports to Congress.[67]

Total Number of NSL Requests. We identified three flaws in the manner in which the FBI records, forwards, and accounts for information about its use of NSLs that affect the accuracy of the FBI's database and reports to Congress on the number of NSL requests issued. They are (1) incomplete or inaccurate information on NSLs issued; (2) field office delays in entering information into ACS, which impedes NSLB's ability to extract and compile data on NSL usage in a timely fashion; and (3) incorrect data in the OGC database.

1) Incomplete or inaccurate information on NSLs issued: During our examination of 293 NSLs in 77 investigative case files, we compared the documents in the case files to the data recorded in the OGC database. We first examined whether NSLs contained in the case files were recorded in the OGC database, and whether the NSLs recorded in the OGC database were contained in the case files. We found that 31 of the 77 case files contained NSLs that were not recorded in the OGC database, and 8 of the case files did not contain NSLs that were recorded in the OGC database. Overall, there were 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" (such as several requests in an NSL for individual telephone numbers or bank accounts) in 212 of the 293 NSLs and compared that to the number of NSL requests recorded in the OGC database for those same national security letters.[68] We found 30 of the 212 NSLs in which the number of NSL requests in the letters differed from the number of NSL requests recorded in the OGC database: 21 contained more NSL requests (194 actual NSL requests versus 36 recorded in the OGC database) and 9 contained fewer NSL requests (18 actual NSL requests versus 38 recorded in the OGC database). Overall, we found 22 percent more NSL requests in the case files we examined than were recorded in the OGC database.

---

[67] 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.

[68] We did not include 55 NSLs that requested information pursuant to FCRAv (full consumer credit reports) because the Department was not required to report that information to Congress during the period covered by our review. We also did not include 12 NSLs for which we could not find a corresponding entry in the OGC database either because the entry (1) was not made; (2) contained typographical errors that prevented us from finding the corresponding entry; or (3) was among those that were lost following a OGC database computer malfunction during the time period of our review.

2) Field delays in entering NSL information: NSLB relies exclusively on the NSL approval ECs to extract information for entry into the OGC database. From 2003 through 2005, some FBI special agents or FBI support personnel in the field did not enter the approval ECs into ACS, the FBI's electronic case management system, in a timely manner. As a result, this information was not in the OGC database when data was extracted for the semiannual reports to Congress. Although this data was subsequently 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 informatiou into the OGC database.[69] In March 2006, the FBI acknowledged to the Attorney General and Congress that NSL data in the semiannual classified reports may not have been accnrate and stated that the data entry delays affected an unspecified number of NSL requests. The FBI indicated that the final numbers of NSL requests may "change slightly should additional data be subsequently reported. . . ."[70] After the FBI became aware of these dclays, it took steps to reduce the impact of the delays to negligible levels for the second half of CY 2005.

3) Incorrect data entries in the OGC database: During our review of the OGC database, we discovered a total of 212 incorrect data entries that caused 477 NSL requests to be erroneously excluded from the Department's semiannual classified reports to Congress. In some cases, the data fields for relevant dates were blank (153 entries affecting 403 NSL requests). In other cases, typographical errors in entering the relevant dates (for example, entering "12/31/203" instead of "12/31/2003") produced entries that were not captured in the reports (59 entries affecting 74 NSL requests). In addition, we determined that the OGC database is programmed to provide a default value of "0" for the number of "NSL requests." Entering a record

---

[69] Most of these (approximately 4,500) were ECPA subscriber information requests. The differences between the NSL requests included in the semiannual classified reports to Congress and the NSL requests included in the OGC database for the other types of NSLs were negligible.

[70] 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; Memorandum for the Attorney General, *Semiannual Report of Requests for Telephone Subscriber or Toll Billing/Electronic Communications Transactional Records Made Pursuant to Title 18, United States Code (U.S.C.), Section 2709, Foreign Counterintelligence/International Terrorism* (March 23, 2006), at 2; and Memorandum for the Attorney General, *Semiannual Report of Requests for Financial Institution and Consumer Identifying Information, and Consumer Credit Reports, Pursuant to Title 15, United States Code (U.S.C.), Section 1681u, for Foreign Counterintelligence/International Terrorism* (March 23, 2006), at 2.

with a "0" entry for NSL requests – which sometimes occurred – is an error, as every NSL generates at least one NSL request. We confirmed that the OGC database includes some records that erroneously indicate "0" items were requested in the NSLs, and thus the database understates the number of NSL requests for those records.

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. However, 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. Based on our analysis of the database and the semiannual classified reports to Congress, the most significant amount of data was lost in 2004. Nonetheless, by comparing the data reflected in the 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.[71]

Total Number of Investigations of Different U.S. Persons and Different non-U.S. Persons. In addition to inaccuracies regarding the total number of NSL requests, we found other inaccuracies in the OGC database that affect the accuracy of the total number of "investigations of different U.S. persons" and "investigations of different non-U.S. persons" that the Department reported to Congress. These included (1) inconsistencies among the NSL approval ECs in the same investigation from which NSLB extracts U.S. person/non-U.S. person data; and (2) incorrect tabulations and data entries in the OGC database. The following are examples of some of these inaccuracies:

1. During investigations, individuals' names may be identified and included in approval ECs in a number of different ways (for example, "John Doe," "Doe, John," "John T. Doe," "J.T. Doe"). The OGC database does not have filters that would enable the FBI to identify NSL requests for the same person in the same investigation.[72]

---

[71] The computer malfunction made it impossible for the OIG to reconstruct electronically the total number of NSL requests issued during the period covered by our review. As a result, the percentages noted in the Classified Appendix for the NSL requests are based on the total number of requests entered in the database made available to the OIG in May 2006. We estimated that as of that time, the OGC database contained approximately 94 percent of the NSL requests made from 2003 through 2005.

[72] NSLB personnel told us that they are aware of this issue and attempt to eliminate these errors by searching the printed reports manually, identifying subject names that appear the same, although not spelled identically, and eliminating those that they are able to determine are the same person.

2. During an investigation, different FBI divisions may generate NSLs seeking information on the same person. Even though these NSLs involve the same person, they are counted separately, resulting in an overstatement of the total number of investigations of different persons. In addition, typographical errors in entries for the requesting offices contribute to the overstatement of these totals.

During our review we found that another default setting in the OGC database results in an understatement of the number of different U.S. persons who were the targets of investigations in which certain types of NSLs were issued. Specifically, we found that from 2003 through 2005, the OGC database contained a default setting of "non-U.S. person" for the investigative subject related to NSL requests for RFPA and ECPA toll billing/electronic communication transactional records. As a result, known or presumed U.S. persons could be misidentified if the default setting was not corrected during entry, resulting in an understatement of the number of investigations of different U.S. persons that used the NSLs. The misidentification and understatement of that number was confirmed in our review of case files in four field offices, during which we identified 26 of 212 approval ECs (12 percent) in which there was a discrepancy regarding the U.S. person status between the OGC database and the case file. All of the instances involved U.S. persons who were erroneously identified in the OGC database as non-U.S. persons. We identified no instances in which non-U.S. persons were erroneously identified as U.S. persons.

In a May 10, 2006, memorandum to the Attorney General, the FBI reported that data in the first annual public report on NSL usage concerning the total number of "different U.S. persons" who were subjects of investigations in which requests for RFPA and ECPA toll billing/electronic communication transactional records were issued in CY 2005 may not be accurate.[73] The FBI explained that the data "could include instances in which one targeted individual was counted more than once" due to limitations of the OGC database. However, in addition to the inaccuracy in the public report disclosed by the FBI, our review of the OGC database, the semiannual classified reports to Congress, and the investigative files in four FBI field offices showed that all of the classified semiannual reports to Congress for 2003 through 2005 contained similar inaccuracies regarding the number of "investigations of different U.S. persons" and "investigations of different non-U.S. persons" that generated NSL requests for RFPA and ECPA toll billing/electronic communication transactional records.

---

[73] Memorandum for the Attorney General, *Annual Report of Total National Security Letter Requests for Information Concerning Different U.S. Persons (Excluding National Security Letters for Subscriber Information) Made Pursuant to the USA PATRIOT Improvement and Reauthorization Act of 2005, Public Law 109-177*, at 2.

The problems with the OGC database, including the loss of data from the OGC database 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 for financial records and NSLs for toll billing/electronic communicatiou transactional records.

II. National Security Letter Requests From 2003 Through 2005

In this section, we describe the FBI's use of NSLs from 2003 through 2005 as documented in the OGC database. As discussed above, the data in the OGC database is not fully accurate or complete and, overall, significantly understates the number of FBI NSL requests. However, 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.

From 2003 through 2005, the FBI issued a total of 143,074 NSL requests (see Chart 4.1, next page).[74] Of that number, [redacted] requests (or [redacted] percent) were made pursuant to the three NSL statutes that are included in the Department's semiannual classified reports to Congress (RFPA, ECPA, and FCRAu). In addition, although the data was not required to be reported to Congress, the OGC database showed that the FBI issued [redacted] NSL requests for consumer full credit reports (FCRAv) during the same period. FBI records show that [redacted].

The number of ECPA NSL requests increased in CY 2004, and then decreased in CY 2005. We determined that the spike in CY 2004 occurred because of the issuance of 9 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.[75] 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

---

[74] As noted earlier, we refer to the number of NSL requests rather than letters because one national security letter may include more than one "NSL request." See Chart 1.1 on page 4.

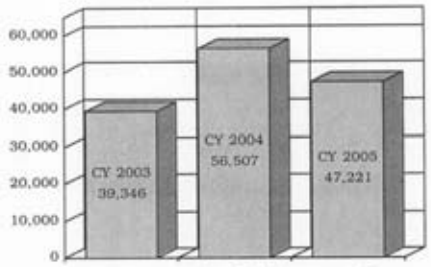
[75] The number of NSL requests we identified significantly exceeds the number reported in the first public annual report issued by the Department because the Department was not required to include all NSL requests in that report. The Department's public report stated that in CY 2005 the FBI issued 9,254 NSL requests for information relating to U.S. persons instead of the [redacted] NSL requests we identified because the public report did not include NSL requests under the ECPA for telephone and e-mail subscriber information, NSL requests under FCRAv for consumer full credit reports, or NSL requests related to "non-U.S. Persons."

statute. The [redacted] used NSL requests, accounting for approximately [redacted] percent of the total, sought records from financial institutions such as banks, credit card companies, and finance companies under the [redacted] authority. The remaining [redacted] percent of the NSL requests were issued pursuant to the [redacted] NSL authorities seeking either financial institution or consumer identifying information [redacted].[76]

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

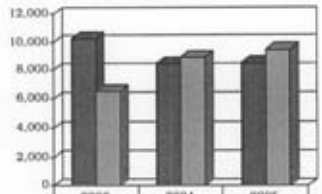
Chart 4.2 (next page) depicts the number of NSL requests relating to investigations of non-U.S. persons and U.S. persons from 2003 through 2005. As shown in Chart 4.2, during the 3 years of our review the balance of NSL requests related to investigations of U.S. persons versus non-U.S. persons shifted. In CY 2003, NSL requests predominantly involved investigations of non-U.S. persons, but by CY 2005 the majority of NSL

[76] A detailed discussion of the FBI's use of each of the four types of NSLs in counterterrorism and counterintelligence investigations is included in the Classified Appendix.

requests were generated from investigations of U.S. persons. However, the number of NSL requests for information generated from investigations of U.S. persons increased by almost 3,000 from 2003 to 2005, while the number of requests generated from investigations of non-U.S. persons decreased by about 1,700. As a result, 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.[77]

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. Persons	10,232	8,494	8,536
U.S. Persons	6,519	8,943	9,475

Source: DOJ semiannual classified NSL reports to Congress

NSL Requests Issued During Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations: The following charts

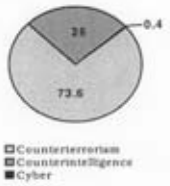
---

[77] 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 [redacted] 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 [redacted] 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.

present the number of NSL requests issued from 2003 through 2005 for different types of investigations.

As shown in Chart 4.3, the majority of NSL requests issued from 2003 through 2005 were issued during counterterrorism investigations. Overall, about 73 percent of the total number of NSL requests issued from 2003 through 2005 were in counterterrorism investigations, and about 26 percent were issued in counterintelligence investigations. Less than 1 percent of the requests were issued in foreign computer intrusion cyber investigations.

CHART 4.3 NSL Requests in Counterterrorism, Counterintelligence, and Foreign Cyber Investigations (2003 through 2005) (U)



Source: FBI-OGC NSL database as of May 2006

We also observed that the use of NSLs in counterterrorism investigations increased between CY 2003 and CY 2005.[78] Chart 4.4 shows the total number of counterterrorism investigations and the number of such investigations in which NSL requests were issued. As shown in Chart 4.4, during the three years the total number of counterterrorism investigations decreased (from [redacted]), but the number of such investigations in which one or more NSLs were used increased from [redacted] in CY 2003 to [redacted] in CY 2005.[79] As a percentage, the use of NSLs in counterterrorism investigations almost doubled during the three years, from 15 percent of the counterterrorism investigations open during CY 2003 to 23 percent during CY 2004 and then to 29 percent in CY 2005. Overall, one or more NSLs were used in about 19 percent of all the counterterrorism investigations that were open at any point from 2003 through 2005.

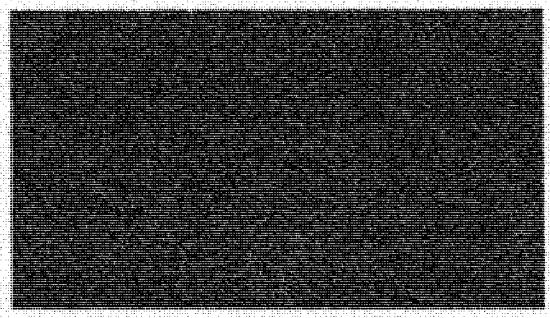
---

[78] Although FBI data identified whether individual NSLs were related to counterterrorism or counterintelligence investigations, the data provided by the FBI regarding counterintelligence investigations open during CY 2003 through CY 2005 was not sufficiently reliable for us to identify the total number of open counterintelligence investigations and the number of those investigations that involved NSLs. Therefore, we are unable to identify any trends in NSL usage in counterintelligence investigations during the period covered by our review.

[79] The total number of investigations open during the three years is less than the sum of the investigations open in each of the years because many investigations remained active during more than one of the years and are counted in each of the years they were open.

CHART 4.4

Counterterrorism Investigations With One or More National Security Letters (2003 through 2005)
[The chart below is classified SECRET]

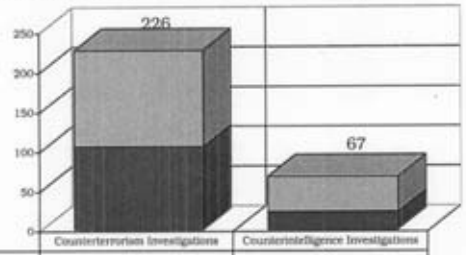


Source: FBI OGC NSL database as of May 2006 and Counterterrorism Division

The FBI's Use of National Security Letters in Different Investigative Stages: As discussed in Chapter Three, one of the most significant changes to the FBI's authority to issue national security letters occurred when the Attorney General issued the NSI Guidelines on October 31, 2003, permitting NSLs to be issued during preliminary investigations. Prior to that time, with limited exceptions, NSLs could be issued only during full investigations. Although the OGC database does not capture the investigative stage at which NSL authority was used, we recorded that information in the 293 NSLs we examined during our field visits. Chart 4.5 illustrates the type of investigation and the investigative stage during which each of the 293 NSLs we examined was issued. Overall, of the 293 NSLs we examined, 77 percent were issued in counterterrorism investigations, 23 percent were issued in counterintelligence investigations, 43.7 percent of the NSLs were issued during preliminary investigations, and 56.3 percent were issued during full investigations.

CHART 4.5

NSL Requests During Preliminary and Full Investigations Identified in Files Reviewed by the OIG (2003 through 2005)



	Counterterrorism Investigations	Counterintelligence Investigations
Full Investigations	121	44
Preliminary Investigations	105	23

Source: Chicago, New York, Philadelphia, and San Francisco FBI Field Division investigative files

CHAPTER FIVE
THE EFFECTIVENESS OF NATIONAL SECURITY LETTERS AS AN INVESTIGATIVE TOOL

III. Introduction

Along with other requirements for OIG review, Congress also directed the OIG to include in our review an examination of the effectiveness of national security letters as an investigative tool, including:

- the importance of information acquired by national security letters to the Department's intelligence activities;
- the manner in which the information acquired from national security letters is collected, retained, analyzed, and disseminated by the Department of Justice, including any direct access to such information provided to any other department, agency, or instrumentality of federal, state, local, or tribal governments or any private sector entity;
- whether and how often the FBI used information obtained from national security letters to produce an "analytical intelligence product" for distribution to, among others, the intelligence community; and whether and how often the FBI provided information obtained from national security letters to law enforcement authorities for use in criminal proceedings.

In this chapter, we address the effectiveness of national security letters as an investigative tool, the manner in which information from national security letters is analyzed and disseminated, and how national security letter-derived information is used.[80] First, we briefly describe how national security letters were used prior to the Patriot Act and what FBI personnel told us about their effectiveness during that period. Next, we describe their use after the Patriot Act, including how national security letters are used to develop information on terrorist or espionage threats. We then describe the various types of FBI analytical intelligence products that use information obtained from national security letters, and how these products are shared within the Department and among other federal agencies. We also discuss how NSL-derived information is disseminated to Joint Terrorism Task Forces and the intelligence community, among others. Next, we address whether and how often the FBI provides information derived from national security letters to law enforcement authorities for use in criminal proceedings.

---

[80] In Chapter Three, we described the FBI's collection and retention of information derived from national security letters.

IV. The Effectiveness of National Security Letters Prior to the Patriot Act

FBI personnel we interviewed who were involved in the use of national security letters prior to the Patriot Act told us that before 2001 NSLs were used infrequently in both counterterrorism and counterintelligence cases. They attributed their infrequent use to several reasons, chief of which was the delay in obtaining approval of the letters. Prior to passage of the Patriot Act, FBI field personnel were not authorized to issue national security letters, and there were significant delays in obtaining Headquarters approval. Because of the lengthy process required to obtain national security letters, FBI personnel said NSLs generally were not viewed as an effective investigative tool.[81]

FBI personnel cited three additional reasons for the ineffectiveness of national security letters in the pre-Patriot Act period. First, under the Attorney General Guidelines in effect at the time, national security letters could be used only during certain phases of investigations. Second, prior to the Patriot Act agents could seek national security letters for telephone and electronic communication transactional records from telephone companies and Internet service providers, records from financial institutions, and information from credit bureaus only upon demonstrating "specific and articulable facts" giving reason to believe that the subject was an "agent of a foreign power" or, in the case of requests for subscriber information, had been in contact with such an agent.[82] FBI officials told us that this predication standard limited the utility of NSLs as an investigative tool.[83]

---

[81] The final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) contained a monograph on terrorist financing that discussed the limited utility of national security letters in the pre-Patriot Act period. The report noted that Minneapolis FBI agents investigating links between a network of money remitters and a terrorist group chose to use tools available in criminal investigations rather than national security letters for two reasons. First, "the FBI could obtain subpoenas almost instantly, whereas NSLs took 6 to 12 months to obtain." Second, national security letters could only be approved by officials at FBI Headquarters. See *Report of the National Commission on Terrorist Attacks Upon the United States*, Terrorist Financing Staff Monograph, Al-Barakaat Case Study (August 21, 2004).

[82] See, e.g., 18 U.S.C. § 2709(b) (2000).

[83] These factors were also noted by a Department official in congressional testimony. The official stated that the predication requirement "put the cart before the horse" because agents could not issue national security letters to establish "specific and articulable facts indicating that the individuals in question were agents of a foreign power." *Material Witness Provisions of the Criminal Code, and the Implementation of the USA PATRIOT Act: Section 505 That Addresses National Security Letter and Section 804 That Addresses Jurisdiction Over Crimes Committed at U.S. Facilities Abroad*: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary, 109th Cong. 9-10 (statement of Matthew Berry, Office of Legal Policy, U.S. Department of Justice).

Several counterterrorism officials cited a third factor for the limited value of national security letters prior to the Patriot Act: the FBI's limited analytical resources to exploit the information received. In the absence of specialized analytical expertise, the FBI relied almost exclusively on case agents to analyze information obtained through national security letters. As we describe below, the FBI's increased analytical capabilities in recent years has changed the perspective of FBI personnel on the use and effectiveness of national security letters.

The former Deputy General Counsel for the FBI-OGC's National Security Law Branch who was responsible for approving national security letters in the late 1990s told us that he considered approximately 300 NSL approval memoranda annually, each of which sought approval of one or more NSLs.[84] He stated that it was necessary to spend significant effort going back and forth with field personnel to evaluate whether there was sufficient evidence to establish the statutory predication that the NSLs related to agents of a foreign power.[85] He noted that the approval process could take as long as one year (an estimate confirmed by other field personnel we interviewed), and because of that FBI case agents would sometimes "give np" and withdraw their requests.

Notwithstanding these limitations, some FBI officials stated that national security letters occasionally were effectively used prior to the Patriot Act. For example, a counterterrorism official in a large FBI field division noted that national security letters were used successfully to identify associates of [redacted].

However, FBI field and Headquarters personnel who have worked with national security letters before and after the Patriot Act believed that their use and effectiveness has significantly increased after the Patriot Act was enacted. For example, one senior counterterrorism official noted that prior to the Patriot Act, counterterrorism investigations were conducted, then closed, when agents could not identify information associating the investigative subject with a terrorist threat. Since the Patriot Act, counterterrorism investigations are closed after the FBI has evaluated information from national security letters, in conjunction with other investigative techniques, which enables the FBI to conclude with a higher level of confidence that the subject poses no terrorism threat. We provide other illustrations of NSLs' use and effectiveness in the sections that follow.

---

[84] Our review of the Department's semiannual classified reports to Congress on NSL usage showed that the FBI issued approximately 8,500 NSL requests in CY 2000 and approximately 7,800 NSL requests in CY 1999.

[85] The former NSLB Deputy General Counsel stated that establishing the statutory predication prior to the Patriot Act was much easier in counterintelligence cases, where the subject was almost always affiliated with a foreign nation.

V. The Effectiveness of National Security Letters as an Investigative Tool in 2003 through 2005

As discussed in Chapter Two, the Patriot Act amendments to national security letter authorities eliminated the requirement that the information sought pertain to a foreign power or an agent of a foreign power, substituting the lower evidentiary threshold that the information sought is relevant to an authorized national security investigation. The amendments also authorized Special Agents in Charge of FBI field divisions to sign national security letters, authority previously extended to only a handful of FBI Headquarters officials. In addition, in October 2003, the Attorney General issued revised Guidelines authorizing the FBI to use national security letters in preliminary investigations, not just in full investigations.[86] Taken together, these three expansions of the FBI's national security letter authorities resulted in significantly greater use of national security letters in counterterrorism, counterintelligence, and foreign computer intrusion cyber investigations.

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

National security letters are one of several investigative techniques available to FBI agents in conducting counterterrorism, counterintelligence, and foreign computer intrusion cyber investigations. Many field agents and Headquarters officials we interviewed said it is difficult to isolate the effectiveness of national security letters in the context of a particular case. They stated that the value of a particular national security letter emerges only over the life of the case.

Nonetheless, in our review of 77 counterterrorism and counterintelligence case files and almost 300 national security letters issued in those cases, and in over 100 interviews of Headquarters and field personnel, we developed information about the importance of national security letters in these investigations during calendar years 2003 through 2005.

FBI Headquarters and field personnel told us that they found national security letters issued pursuant to the Electronic Privacy Communications Act (ECPA), the Right to Financial Privacy Act (RFPA), and the two authorities in the Fair Credit Reporting Act (FCRA) to be effective in both counterterrorism and counterintelligence investigations, many calling them "indispensable" or "our bread and butter."

---

[86] Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines)(October 31, 2003).

1. Principal Uses of National Security Letters

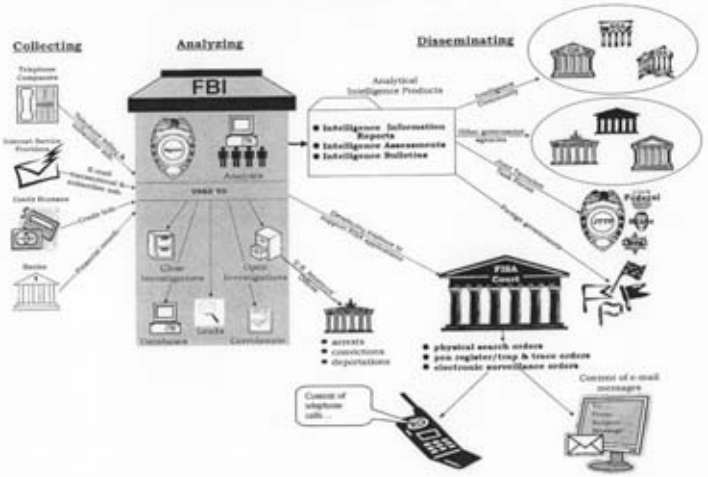
FBI personnel reported that they use national security letter authorities to accomplish one or more of the following objectives:

- Establish evidence to support FISA applications for electronic surveillance, physical searches, or pen register/trap and trace orders;
- Assess communication or financial links between investigative subjects or others;
- Collect information sufficient to fully develop national security investigations;
- Generate leads for other field divisions, members of Joint Terrorism Task Forces, or 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 these key uses of national security letters.

DIAGRAM 5.1

How the FBI Uses National Security Letters



2. The Value of Each Type of National Security Letter

While details concerning the FBI's use of national security letters in particular investigations are classified, our examination of investigative files and interviews of case agents and supervisors assigned to counterintelligence and counterterrorism squads revealed that information obtained from ECPA, RFPA, and FCRA national security letters has contributed significantly to many counterterrorism and counterintelligence investigations. We describe specific examples of the importance of information obtained from the use of each type of national security letter authority below.

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

In counterterrorism investigations, telephone toll billing records and subscriber information and electronic communication transactional records obtained pursuant to ECPA national security letters enables FBI case agents to connect investigative subjects with particular telephone numbers or e-mail addresses. It also allows the FBI to connect terrorism subjects and terrorism groups with each other. Analysis of subscriber information obtained from national security letters for particular 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 national security letter.

Many Headquarters officials as well as case agents and supervisors in the four field offices we visited told 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. For example, to obtain FISA orders the FBI must establish [redacted]. ECPA national security letters for subscriber information routinely are used to confirm this required element and to otherwise develop evidence to support orders from the FISA Court. FISA court orders for electronic surveillance may authorize the FBI to collect the content of communications, information the FBI cannot obtain using NSLs.

The following text box provides examples of the use of ECPA national security letters in counterterrorism and counterintelligence investigations.

Use of Telephone Toll Billing Records and Subscriber Information Obtained by National Security Letters in Counterterrorism and Counterintelligence Cases

- Through national security letters, an FBI field office obtained telephone toll billing records and subscriber information about an investigative subject in a counterterrorism case. The information obtained identified the various telephone numbers with which the subject had frequent contact. Analysis of the telephone records enabled the FBI to identify a group of individuals residing in the same vicinity as the subject. The FBI initiated investigations on these individuals to determine if there was a terrorist cell operating in the city.
- FBI agents told us that national security letters were critical in a counterintelligence investigation that led to a conviction of a representative of a foreign power. The subject owned a company in the United States and traveled to a foreign country at the behest of a foreign intelligence service. In addition, the subject had been collecting telephone records and passing the records to a foreign intelligence officer located in the United States. Through toll billing records obtained from national security letters, the FBI was able to demonstrate that the foreign country's U.S.-based intelligence officer was in contact with the subject.
- After learning from the intelligence community that a suspected terrorist was using a particular telephone number and e-mail account, an FBI field division obtained telephone toll billing and subscriber information on the accounts. The NSLs identified that the subject was in touch with an individual who had been convicted of federal charges.
- In a counterintelligence investigation, telephone toll records obtained through national security letters revealed that, contrary to an FBI source's denials, the source was continuing to contact a foreign intelligence officer by telephone.

In counterintelligence investigations, analysis of telephone and Internet transactional records obtained through national security letters also is valuable, enabling the FBI to identify a subject's contacts with an agent of a foreign power and with individuals who may be in a position to provide access to prohibited technologies. [redacted]

b. Financial records

Financing is critical to terrorist organizations, and 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 their spending patterns. Analysis of this data can also 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. However, analysis of financial records in counterterrorism investigations may be complex and time-consuming because investigative subjects often engage in legitimate businesses that disguise their terrorist affiliations.

FBI case agents and supervisors of counterintelligence cases told us that RFPA national security letters have provided vital information in their investigations. For example, NSL-derived information has demonstrated investigative subjects' access to unexplained sources of income, transactions with foreign government officials, and acquisition of prohibited technologies.

The following text box provides examples of the use of the RFPA national security letters in two counterterrorism investigations.

Use of Financial Records Obtained by National Security Letters in Counterterrorism Investigations

- The FBI conducted a multi-jurisdictional counterterrorism investigation of convenience store owners in the United States who allegedly sent funds to known Hawaladars (persons who use the Hawala money transfer system in lieu of or parallel to traditional banks) in the Middle East. The funds were transferred to suspected Al Qaeda affiliates. The possible violations committed by the subjects of these cases included money laundering, sale of untaxed cigarettes, check cashing fraud, illegal sale of pseudoephedrine (the precursor ingredient used to manufacture methamphetamine), unemployment insurance fraud, welfare fraud, immigration fraud, income tax violations, and sale of counterfeit merchandise.

  The FBI issued national security letters for the convenience store owners' bank account records. The records showed that two persons received millions of dollars from the subjects and that another subject had forwarded large sums of money to one of these individuals. The bank analysis identified sources and recipients of the money transfers and assisted in the collection of information on targets of the investigation overseas.

- The subject of a counterterrorism investigation was allegedly involved in narcotics trafficking. When analysis of telephone records revealed that an individual was in telephone contact with the subject, the FBI issued RFPA NSLs for that individual's bank account records. Examination of the bank records revealed no significant ties to the subject and in the absence of any information linking this individual to terrorist activities, further investigation was terminated.

c. Consumer credit records

The original FCRA NSL statute authorizes the FBI to obtain information about financial institutions from which an individual has sought or obtained credit and consumer identifying information limited to the subject's name, current address and former addresses, places of employment, and former places of employment. The Patriot Act amendment to the FCRA now authorizes the FBI to obtain through national security letters consumer full credit reports, including records of individual accounts, credit card transactions, and bank account activity. Information secured from both types of FCRA national security letters assist case agents because they 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. The supervisor of a counterterrorism squad told us that FCRA NSLs enable the FBI to see "how their investigative subjects conduct their day-to-day activities, how they get their money, and whether they are engaged in white collar crime that could be relevant to their investigations."

The following text box provides examples of the use of both types of FCRA national security letters in counterintelligence and counterterrorism investigations.

Use of Consumer Credit Bureau Records Obtained by National Security Letters in Counterintelligence and Counterterrorism Investigations

- During a counterintelligence investigation, the FBI issued an FCRA NSL seeking financial institution and consumer identifying information about an investigative subject who the FBI was told had been recruited to provide sensitive information to a foreign power. The information obtained from the NSL assisted the FBI in eliminating concerns that the subject was hiding assets or laundering funds or that he had received covert payments from the foreign power.
- In the aftermath of Hurricane Katrina, many subjects of a major FBI counterterrorism investigation moved from areas affected by the disaster. To assist in locating these subjects, the FBI served FCRA NSLs for updated credit card information on the subjects. The information revealed the subjects' credit card activity in a major U.S. city and several foreign countries.
- The FBI initiated an investigation of an individual who was identified during the arrest of a known terrorist in a foreign country. After obtaining a credit card number used by the subject, the FBI served an NSL to obtain a consumer full credit report. The report showed that the subject had relocated to another U.S. city. The FBI's investigation was transferred to the FBI division in that city.

B. Analysis of Information Obtained From National Security Letters

The FBI performs various analyses and develops different types of analytical intelligence products using information from national security letters.

1. Types of Analysis

The review of information derived from national security letters is initially performed by the case agents who sought the national security letters. In counterterrorism investigations, once the case agents confirm that the response to the national security letter 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.

In some field offices, case agents are required to formally document their receipt of information from national security letters, including the date the information was received; the subject's name, address, and Social Security number; and a summary of the information obtained. This document then is electronically uploaded into the FBI's principal investigative database, the Automated Case Support (ACS) system. Once the data is available electronically, other case agents can query ACS to identify information obtained from national security letters that may pertain to their investigations.

After the case agent's initial analysis, analysts assigned to counterterrorism, counterintelligence, or cyber squads in the FBI's field divisions can use the NSL-derived information. The Counterterrorism and Counterintelligence Divisions in FBI Headquarters also conduct communication and financial analyses of NSL-derived information from different national security investigations.

Beginning in mid-2003, FBI field offices established Field Intelligence Groups (FIGs) as part of the Counterterrorism Division's Office of Intelligence. These squads later were moved to the FBI's Directorate of Intelligence. The FIG squads are staffed principally with intelligence analysts, language analysts, physical surveillance specialists, and field agents. FIG squads generate detailed analyses of intelligence information, some of which is derived from national security letters.

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 a national security letter, the data is uploaded into Telephone Applications, a specialized database that can be used to analyze the calling patterns of a subject's telephone number.

The FBI also places NSL-derived information into 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. This FBI database contains over 560 million FBI and other agency records; information obtained from state, local and foreign law enforcement agencies; and open source data. The database can be accessed by nearly 12,000 users, including FBI agents and analysts and members of Joint Terrorism Task Forces.[87] Information derived from national security letters that is uploaded into ACS and into the Telephone Applications database is periodically uploaded to IDW.

FBI policy requires that case agents in counterterrorism investigations conduct a financial analysis of the investigative subject's financial activities. Some large FBI field divisions have dedicated squads, such as terrorist financing squads, to assist agents in analyzing the financial aspects of the subject. These squads may include specialists from outside of the FBI, such as the Defense Criminal Investigative Service or the Internal Revenue Service, who provide expertise in specific financial areas.

Like telephone call analysis, a review of financial records obtained through national security letters may show in a counterintelligence case that the subject is in contact with a foreign embassy or other foreign establishment or with other individuals known to be involved in intelligence activities. This analysis may reveal the names of people who have access to bank accounts, funds that have been transferred in and out of the accounts, and where the funds were transferred.

"Link analysis" is one of the principal analytical intelligence products generated by FIG analysts that rely on information derived from all types of national security letters used by the FBI during the period covered by our review. Link charts illustrate the telephone numbers, Internet e-mail addresses, businesses, credit card transactions, addresses, places of employment, banks, and other data derived from the NSLs, as well as information derived from other investigative tools and open sources. FBI agents and analysts develop link analyses in both counterterrorism and counterintelligence investigations, often integrating the results of multiple NSLs on the subjects of multiple FBI investigations.

Analytical intelligence products based on information obtained from national security letters integrate communication and financial information

---

[87] *FBI Oversight*: Hearing Before the Senate Comm. on the Judiciary, 109th Cong. 6 (2006) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigations.

on particular investigative subjects and their associates. For example, national security letter-derived data reflecting telephone activity on a cluster of dates may correspond with wire transfer information obtained from national security letters served on financial institutions. In one such example, this type of information was integrated to support investigations of a threat to a major U.S. city. FIG analysts combined related information from different investigations throughout the FBI to identify contacts and financial transactions between subjects of the investigation.

2. Formal Analytical Intelligence Products

Information derived from national security letters may also 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.

However, FBI counterintelligence and counterterrorism personnel told us that FBI practice and policy discourage reference to the source of the information discussed in these products in order to protect the FBI's sources and methods. Nonetheless, field personnel we interviewed, including intelligence analysts and financial analysts, told us that the following types of analytical products frequently contain information derived from national security letters, particularly if they are based on information derived from FISA authorities (electronic surveillance, physical searches, or pen register/trap and trace devices). As noted above, one of the most important uses of national security letters is to develop evidence to support FISA applications. Since FISA applications for electronic surveillance must contain evidence [redacted].

The following are examples of FBI analytical intelligence products that use information obtained from NSLs.

- **Intelligence Information Reports**

An Intelligence Information Report (IIR) contains "raw intelligence," which may include information from only one source or one area that has not been fully "vetted" or verified. Headquarters and field personnel told us that FBI analysts sometimes use raw data obtained from national security letters – such as telephone numbers or Internet e-mail account information – in preparing IIRs. For example, if the initial analysis of telephone toll records and subscriber information reveals important ties between a known terrorist and others, the analyst may generate an IIR quickly if the geographic location of the subject is known. In this circumstance, the IIR

would be based on telephone toll billing records information combined with information derived from other investigative tools, such as physical surveillance. Rather than taking time to verify the information, the analyst may determine that it is important to issue an IIR to alert other FBI divisions, state and local law enforcement authorities, and other members of the intelligence community of the raw intelligence. Similarly, if NSLs accessing bank records show that a subject being investigated for espionage has used certain techniques, the FBI would consider communicating a description of these techniques in an IIR.

FIG analysts prepare the IIRs, which are uploaded into an FBI database and distributed to all FBI personnel, to allow other offices to connect information in their files to the information in the IIR. The IIRs also are sent to the Criminal Investigative, Counterterrorism, Counterintelligence, and Cyber divisions at FBI Headquarters where a determination is made whether to distribute them more broadly in the intelligence community. In addition, IIRs involving criminal matters may be sent to other law enforcement agencies. One FIG supervisor of a large field office we visited during the review stated that his office published 700 IIRs in CY 2005, the majority generated by the division's counterintelligence squads. Overall, the FBI has generated over 20,000 IIRs from September 2001 to September 2006.[88]

- **Intelligence Assessments**

An Intelligence Assessment is a finished intelligence product developed by the FIGs that provides information on developing crime problems and emerging developments and trends regarding national security threats. Unlike an IIR that contains raw data, Intelligence Assessments use empirical data, known intelligence information, and information from national security letters to draw conclusions and recommendations. These recommendations can provide direction to specific FBI squads or programs.

Intelligence Assessments are prepared for all FBI investigative programs, including counterterrorism and counterintelligence, and for special events. Intelligence analysts we interviewed told us that while they use information obtained through national security letters to help create Intelligence Assessments, they do not attribute information in the assessment to NSLs. For example, intelligence analysts told us that in developing various Intelligence Assessments they used multiple NSLs to assess threats to a major U.S. city, risks associated with terrorists' use of certain weapons of mass destruction, the presence of foreign intelligence officers in major U.S. cities, and efforts by foreign intelligence officers to target corporate officials in order to influence U.S. policy. The assessments

---

[88] See www.fbi.gov.

relied in part on information developed from ECPA, RFPA, and FCRA national security letters.

- **Intelligence Bulletins**

An Intelligence Bulletin is a finished intelligence product that contains general information on a subject or topic as opposed to case-specific intelligence that would be included in an IIR. Intelligence Bulletins generally are prepared by agents or analysts serving on the FIG squads and may be distributed within the Department, to law enforcement authorities, or to other members of the intelligence community.

Intelligence analysts we interviewed told us that while they use information obtained through national security letters to help create Intelligence Bulletins, they do not attribute information in the Bulletins to NSLs. Examples of Intelligence Bulletins that relied on NSL-derived information include products describing bulk purchases of cell phones, developments in the leadership of terrorist groups in U.S. cities, the potential for terrorist recruitment using the Internet, and manufacturers of component parts for explosives being used in Iraq.

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 the intelligence community.[89] For example, the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI) Guidelines provide:

> The general principle reflected in current laws and policies is that information should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. Under this general principle, the FBI shall provide information expeditiously to other agencies in the Intelligence Community, so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions.[90]

In addition, four of the five national security letter authorities expressly permit dissemination of information derived from national security

---

[89] See, e.g., Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003).

[90] NSI Guidelines, § VII(B).

letters to other federal agencies if the information is relevant to the authorized responsibility of those agencies and is disseminated pursuant to the applicable Attorney General Guidelines.[91]

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. According to the FBI officials we interviewed, the nature and extent of dissemination depended upon several factors, including the importance and specificity of the information and whether the NSL data was integrated into formal analytical intelligence products. 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.[92] 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.

Based on our interviews of Headquarters and field personnel and a questionnaire distributed to counterterrorism and counterintelligence squads in Headquarters and field divisions, we learned that the principal entities outside the Department to whom information derived from national security letters was disseminated were members of the intelligence community and Joint Terrorism Task Forces.

Department Components: The NSI Guidelines authorize the FBI to share information obtained through intelligence activities conducted under the Guidelines with other components of the Department of Justice.[93] Information derived from national security letters is shared with United

---

[91] 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.

[92] The supervisor of a FIG squad explained that when FIG analysts receive raw NSL-derived information, such as telephone or bank records, their analyses based on this data are uploaded into ACS and provided to operational squads in the form of electronic communications. These tactical analyses may later become part of finished intelligence products, such as Intelligence Bulletins or Intelligence Assessments, that FBI Headquarters may authorize for dissemination to other members of the intelligence community. Since members of the FIG do not reference what information was derived from NSLs, the source of the information would not be associated with the data because it is assimilated into a finished intelligence product.

[93] NSI Guidelines, VII(B)(2).

States Attorneys' Offices (described below), the Drug Enforcement Administration, the Federal Bureau of Prisons, and other Department components, including components whose personnel serve on Joint Terrorism Task Forces, such as prosecutors and intelligence research specialists.

Joint Terrorism Task Forces: Joint Terrorism Task Forces (JTTFs) are composed of representatives of federal, state, and local law enforcement agencies who respond to leads, investigate, make arrests, provide security for special events, and collect and share intelligence related to terrorist threats.[94] Some task force members are designated Task Force Officers, some of whom obtain the necessary clearances to obtain access to FBI information, including information derived from national security letters and other investigative techniques. These Task Force Officers also are authorized to access information stored in FBI databases such as ACS, the specialized application for telephone data, and IDW which, as noted above, contain information derived from NSLs. Task Force Officers who obtain the required security clearances and sign access agreements are issued accounts to access these databases (with the exception of case information to which access was restricted due to special sensitivities). Consequently, Task Force Officers with approved user accounts are able to access databases that house raw data derived from NSLs. In addition, Task Force Officers have access to formal analytical products derived, at least in part, from national security letters and other information. However, Task Force Officers are not permitted to share this information with their host agencies unless specifically authorized in memoranda of understanding between the FBI and the host agency.

Other Federal Agencies: The Attorney General's NSI Guidelines authorize the FBI to share information obtained through intelligence activities conducted under the Guidelines with other federal law enforcement agencies and the Department of Homeland Security.[95] Since many federal agencies are represented on JTTFs, the JTTFs are a significant information-sharing mechanism for information derived from national security letters as well as other investigative techniques.[96] In addition, several FBI field divisions told us that they disseminated information

---

[94] Each of the FBI's 56 domestic field divisions contains at least one JTTF, and as of March 2005 the FBI operated JTTFs in 100 U.S. cities.

[95] NSI Guidelines, VII(B)(3).

[96] For example, members of the JTTF in a major FBI field division include representatives from the United States Attorney's Office, United States Marshals Service, United States Postal Service, United States Secret Service, Department of Homeland Security, Federal Protective Service, United States Coast Guard, Department of Defense, Central Intelligence Agency, as well as representatives from state and local law enforcement, including the state police and the city police department.

derived from NSLs to the Department of Energy and the Department of Commerce in connection with counterintelligence investigations.

During our site visits to four FBI field offices, we reviewed examples of documented dissemination of IIRs, Intelligence Bulletins, and Intelligence Assessments to other federal agencies. For example, case agents on counterintelligence squads disseminated NSL-derived information to the Commerce Department's Export Control Agency to identify products on an export control list. Case agents on counterterrorism squads disseminated NSL-derived information to the Immigration and Customs Enforcement branch in the Department of Homeland Security related to the investigation of potential immigration charges.

Members of the Intelligence Community: The NSI Guidelines authorize the FBI to share information covered by various memoranda of understanding with members of the intelligence community.[97] Consequently, FBI analytical products that contain information from national security letters are disseminated to other members of the intelligence community. FBI field offices told us that they disseminated information derived from national security letters to the Central Intelligence Agency, National Reconnaissance Office, Defense Intelligence Agency, Naval Criminal Investigative Service, Air Force Office of Special Investigations, and the National Security Agency. As noted above, these analytical products normally do not reference the source of the information used to produce the product.

Private Sector Entities: Together with threat information derived from other investigative tools, information from national security letters is included in threat advisories that are communicated to private sector entities. FBI officials in the four divisions we visited during the review told us that they brief members of the private sector on terrorist threats or other threats associated with special events, such as the Olympics or the World Series. These briefings may advise the security officials of private companies of the nature of the threat, but they do not communicate details of pending investigations or what investigative tools were used to identify and assess the severity of the threat.

Foreign Governments: The NSI Guidelines authorize the FBI to share information obtained through intelligence activities under the Guidelines, which include information from national security letters, with foreign authorities under specified circumstances when the dissemination is in the interest of the United States.[98] Information derived from national security letters can also generate leads that are passed on to foreign government counterparts.

---

[97] NSI Guidelines, VII(B)(3).

[98] NSI Guidelines, VII(B)(6).

Dissemination of information to foreign governments during most of the period covered by our review was handled by the Designated Intelligence Disclosure Officials (DIDO) within the Directorate of Intelligence at FBI Headquarters.[99] Personnel in several field offices told us that they proposed the dissemination of information derived from national security letters to foreign governments from 2003 through 2005. For example, the Directorate of Intelligence approved the request of an FBI field division to provide information to a foreign intelligence service about the possible association of two non-U.S. telephone numbers to terrorist activities and to request assistance in obtaining subscriber information about the two telephone numbers.

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

Information from national security letters most often is used for intelligence purposes rather than for criminal investigations. In some instances, however, NSL-derived information, when combined with other information, is useful in criminal investigations and prosecutions. However, our review could not determine how often that occurs because the FBI does not maintain such records, and NSL-derived information is not specifically labeled as such when it is provided to law enforcement authorities.

In this section, we describe the ways in which the FBI provides information derived from NSLs to law enforcement authorities both through routine information sharing with United States Attorneys' Offices (USAOs) and in connection with specific criminal investigations and prosecutions. We also give specific examples of instances in which the FBI provided law enforcement authorities information derived from national security letters that was used in criminal proceedings.

1. Routine Information Sharing With United States Attorneys' Offices

Information obtained from national security letters and analytical products derived from this information are routinely shared with prosecutors in the USAOs, although the source and details of the information may not be readily apparent to the prosecutors. The information is shared with USAOs to determine if criminal or other charges may be brought against individuals who are subjects of FBI counterterrorism investigations.[100]

---

[99] Only Designated Intelligence Disclosure Officials are authorized to decide that intelligence information may be released to foreign governments. The FBI Director is a DIDO and has delegated DIDO authority to other senior FBI officials.

[100] Following the September 11 terrorist attacks, the Department implemented an anti-terrorism plan that directed the commitment of all available resources and manpower

In November 2002, the Attorney General directed the United States Attorneys and the Criminal Division to review counterterrorism intelligence investigative files to determine whether they contained information that would support criminal proceedings. In June 2004, the Deputy Attorney General directed the United States Attorneys to identify all open full field FBI counterterrorism investigations that the USAOs or the local FBI field offices believed may relate to certain current threats. In consultation with FBI field offices, the USAOs were directed to determine "if there exists a potential criminal disruption option by identifying any criminal charges that appear to be available now or could be available imminently with additional investigation."[101]

Through such routine interactions with the FBI, terrorism prosecutors are familiar with the progress of counterterrorism investigations being conducted in their districts. While it would be unlikely that FBI case agents would need to attribute the fruits of their investigative activities to particular investigative techniques – such as national security letters – in routine briefings terrorism prosecutors may learn that national security letters were used and, in significant briefings, likely learn of the fruits of the technique. In addition, 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.[102]

(cont'd.)

to address efforts to detect and prevent terrorism. Two important aspects of the plan were the establishment of Anti-Terrorism Advisory Councils (ATACs) within each judicial district and the expansion of Joint Terrorism Task Forces. ATACs were directed to convene federal law enforcement agencies and state and local law enforcement officials who, together, would constitute the ATAC for each district. The ATACs were charged with coordinating "the dissemination of information and the development of prosecutive strategy" about suspected terrorists and "implement the most effective strategy for incapacitating them." See Memorandum from John Ashcroft, Attorney General, U.S. Department of Justice, to All United States Attorneys, *Anti-Terrorism Plan* (Sept. 17, 2001).

[101] Memorandum from James B. Comey, Deputy Attorney General, U.S. Department of Justice, to United States Attorneys and Anti-Terrorism Advisory Council Coordinators (June 25, 2004), at 2.

[102] Intelligence research specialists in USAOs assist the ATACs in coordinating anti-terrorist activities by, among other activities, generating analyses of the relevance and reliability of threat information and investigative leads. See Office of the Inspector General, U.S. Department of Justice, *A Review of United States Attorneys' Offices Use of Intelligence Research Specialists* (December 2005).

In some districts, the ATAC Coordinators and intelligence research specialists are full members of the district's Joint Terrorism Task Force. In those circumstances, these Department personnel have access to FBI databases. As noted above, several FBI databases contain either raw data obtained from NSLs or analytical products derived from them.

In the course of these file reviews, terrorism prosecutors and intelligence research specialists assigned to the USAOs may identify gaps in the data collected from all investigative techniques, including NSLs, and may suggest that additional NSLs be issued to fill these gaps. For example, if an analyst learns that the subject has received funds from a foreign country, the analyst may suggest to the case agent that RFPA NSLs be issued to obtain financial records about the subject. If the subject is suspected of money laundering or violations of the Export Control Act, the analyst may suggest that the agent issue FCRA NSLs to learn more about the subject's consumer credit transactions.

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

When criminal prosecutions are pursued, information from national security letters may also be used in criminal proceedings. Information derived from national security letters may produce evidence for the prosecution's case in chief, for example by identifying communications or financial networks indicative of criminal conspiracy or material support for terrorism.[103] It may also provide evidence that persuades the subject to

---

[103] In June 2006, the Department's Counsel for the Office of Intelligence Policy and Review (OIPR) asked the Department's Office of Legal Counsel (OLC) to render an opinion on whether the FBI is required under the Foreign Intelligence Surveillance Act (FISA) to obtain Attorney General approval prior to disseminating certain information for law enforcement purposes that is developed from national security letters. The FBI and the Department's Criminal Division Counterterrorism Section submitted legal analyses and their positions to OLC in conjunction with this request. Specifically, the Counsel for OIPR asked whether Attorney General approval is required under the FISA before the FBI seeks to obtain a grand jury subpoena based on the results of NSLs that were issued for telephone toll records on telephone numbers identified through its use of FISA authorities. The FISA requires that information obtained through the use of orders for electronic surveillance, physical searches, and pen registers/trap and trace devices

> shall not be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may be used in a criminal proceeding with advance authorization of the Attorney General.

50 U.S.C. §§ 1806(b)(electronic surveillance), 1825 (c)(physical searches), 1845(b)(pen registers/trap and trace devices). The Counsel also asked whether the term "criminal proceeding" means all federal grand jury proceedings, including the issuance or grand jury subpoenas, as well as search warrants, indictments, and trials. In late 2006, after receiving the views of relevant entities, OLC referred the question to the Department's National Security Division for a determination of the best policy approach that comports with the FISA. In February 2007, NSD contacted the FBI and other members of the intelligence community for the purpose of meeting to determine the best policy approach. If Attorney General approval were needed, the Counsel believes and FBI officials confirmed that there would be significant operational implications for the ability of prosecutors and FBI agents to quickly follow leads generated from FISA collection.

cooperate with the government and provide information on other terrorists or other illegal activity. 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. Moreover, when sharing intelligence with law enforcement authorities, FBI agents do not typically refer to the investigative technique that was used to gather information.

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.[104] However, we attempted in another way to obtain a rough sense of how often the FBI provided NSL-derived information to federal law enforcement authorities for use in criminal proceedings by collecting information that is indicative of such use. Specifically, we asked FBI field personnel to identify instances in which they referred targets of national security investigations to law enforcement authorities for prosecution and whether in those instances they shared information derived from national security letters with law enforcement authorities.[105] We learned from the responses that in addition to the routine sharing of information noted above, 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.[106] 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).

---

[104] By contrast as noted above, when FBI case agents obtain information from the use of FISA authorities, the information is marked or tagged so that its derivation is clear.

[105] In the absence of a tagged digital record or a centralized repository reflecting instances in which information derived from national security letters is provided to law enforcement authorities for use in criminal proceedings, FBI attorneys suggested that we collect data on how often case agents referred targets of national security investigations to law enforcement authorities for possible prosecution. These referrals would capture the universe of investigations in which national security letters were authorized to be issued, and the results of information derived from national security letters issued in these investigations may have been shared with prosecutors, even if the source of the information was not explicitly noted.

[106] By contrast, case agents and supervisors assigned to counterintelligence squads said that there is rarely a criminal nexus in these investigations, and therefore information derived from national security letters would typically not be provided to law enforcement authorities.

We also asked FBI field offices to identify examples from the referrals to law enforcement authorities of the particular matters in which information from national security letters was used in criminal prosecutions.[107] Although the field offices that provided data on such referrals were unable to state in what percentage of these referrals they used NSLs, they provided examples of the use of NSLs in these proceedings, such as the following:

a. Counterintelligence Case No. 1

A counterintelligence investigation focused on the possible involvement of the subject in exporting sensitive U.S. military technology to a foreign country. Multiple national security letters were issued to obtain information that enabled the FBI to identify the subject's role in exporting these technologies. The FBI shared the NSL-derived information with the Internal Revenue Service, which led to the initiation of a grand jury that returned money laundering charges against the subject. The FBI also shared the NSL-derived information with the Department of Homeland Security and the Department of Commerce Office of Export Enforcement. The FBI's investigation led to guilty pleas for 22 violations of the Arms Export Control Act and brokering the export of sensitive technologies without the required government licensing approval.

b. Counterterrorism Case No. 1

Information provided to the FBI from the intelligence community suggested that a high-value detainee who was to be incarcerated at Guantanamo Bay had used an e-mail account. The FBI issued national security letters to obtain e-mail transactional information about the user's e-mail account, which led to additional national security letters seeking telephone toll records and subscriber information on the subject and the subject's friends and associates. Information derived from one of the national security letters established a connection between the subject and the subject of another FBI investigation. The latter individual was later convicted of providing material support to terrorism.

c. Counterterrorism Case No. 2

An FBI field office issued national security letters to ascertain the investigative subject's financial dealings. The information from the national security letters suggested bank fraud activity. A federal grand jury was

---

[107] One field division provided an approximation of the number of times it used NSL-derived information in criminal proceedings. That division stated that it used NSL-derived information in approximately 105 criminal proceedings from 2003 through 2005. The division reported that NSLs were used only in terrorism-related criminal proceedings, not in any espionage-related criminal proceedings.

convened, and grand jury subpoenas were issued to obtain financial records for use in the criminal trial. The investigative subject and his wife were convicted of bank fraud, making false statements, and conspiracy.

d. Counterterrorism Case No. 3

An FBI field division used information from national security letters in an investigation of individuals accused of being members of [redacted].

VI. Conclusion

FBI Headquarters and field personnel told us that they believe national security letters are indispensable investigative tools that serve as building blocks in many counterterrorism and counterintelligence investigations. In further addressing the question of the effectiveness of NSLs, we considered the investigative and analytical objectives for using NSLs. Headquarters and field personnel told us that the principal objective of the most frequently used type of NSL – ECPA NSLs seeking telephone toll billing records, electronic communication transactional records, or subscriber information (telephone and e-mail) – is to develop evidence to support applications for FISA orders. NSLs also are used in counterterrorism and counterintelligence investigations to determine how and when subjects are communicating with others, their sources of funds and means of transferring funds, and how they are financing their activities. FBI agents and analysts use information derived from NSLs to determine if further investigation is warranted; to generate leads for other field offices, Joint Terrorism Task Forces, or other federal agencies; and to corroborate information developed from other investigative techniques.

The FBI generates a variety of analytical intelligence products using information derived from NSLs, including Intelligence Information Reports, Intelligence Assessments, and Intelligence Bulletins. Information derived from NSLs is stored in various FBI databases, shared within the Department and with Joint Terrorism Task Forces, and disseminated to other federal agencies and the intelligence community. The FBI also provides information from NSLs to law enforcement authorities for use in criminal proceedings.

CHAPTER SIX
IMPROPER OR ILLEGAL USE OF NATIONAL SECURITY LETTER AUTHORITIES

The Patriot Reauthorization Act also directed the OIG to describe any "improper or illegal use" of the FBI's authorities to issue national security letters. In this chapter, we report our findings on improper or illegal use of the authorities that were identified by the FBI, as well as instances we discovered during our review of a sample of FBI investigative files. We also describe other uses of national security letter authorities in which FBI field personnel deviated from internal FBI policies related to NSLs that are designed to ensure appropriate FBI supervisory review and compliance with statutory authorities and Attorney General Guidelines.

In the course of our review, we identified a variety of instances in which the FBI used national security letters contrary to statutory limitations, Attorney General Guidelines, or internal FBI administrative guidance or policies. In addition to these incidents, we identified certain practices where the legality or propriety of the use of national security letters was unclear due to inadequate FBI recordkeeping practices that did not generate an audit trail that would enable us to determine if the letters were duly authorized. For example, FBI Headquarters has no policy requiring the retention of signed copies of national security letters issued by the FBI or signed copies of FBI requests for the same types of information without using an NSL, and three of the four field offices we visited did not maintain signed copies of these letters and other requests. This made it impossible for us to determine whether national security letters were signed by appropriate FBI officials, to confirm the precise information requested in the letters, or to determine the number and nature of the other types of requests.[108]

The instances of improper or illegal use of NSL authorities generally fell into the following categories:

- Issuing national security letters when the investigative authority to conduct the underlying investigation had lapsed;
- Obtaining telephone toll billing records and e-mail subscriber information concerning the wrong individuals;
- Obtaining information that was not requested in the national security letter;

---

[108] If national security letters were not signed by Special Agents in Charge or specially delegated senior Headquarters officials, this would be a violation of the national security letter statutes, the Attorney General's NSI Guidelines, and internal FBI policy.

- Obtaining information beyond the time period referenced in the national security letter;
- Issuing Fair Credit Reporting Act (FCRA) national security letters seeking records that the FBI was not authorized to obtain through an NSL in the pending investigation under the referenced statute, such as issuing FCRAv consumer full credit report national security letters in counterintelligence investigations;
- Issuing improper requests under the statute referenced in the NSL, such as issuing an ECPA national security letter seeking an investigative subject's educational records, including applications for admission, emergency contact information, and associations with campus organizations;
- Obtaining telephone toll billing records by issuing "exigent letters" signed by a Counterterrorism Division Unit Chief or subordinate personnel rather than by first issuing duly authorized national security letters pursuant to the ECPA NSL statute; and
- Issuing national security letters out of "control files" rather than from "investigative files" in violation of FBI policy.

In Section I, we discuss incidents triggered by the use of NSLs that were reported by field agents to the FBI's Office of the General Counsel (FBI-OGC) as possible violations of intelligence authorities that should be reported to the Intelligence Oversight Board (IOB). In Section II, we discuss similar types of incidents and other incidents that were not reported by FBI personnel to FBI-OGC but were identified by the OIG during our site visits to four field divisions. In Section III, we discuss the improper or illegal uses of national security letter authorities that we identified were committed by FBI Headquarters Counterterrorism Division personnel. In Section IV, we describe instances identified by the OIG in which we found that FBI employees failed to adhere to internal controls on the exercise of national security letter authorities.

In evaluating these matters, it is 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.

I. Possible IOB Violations Arising from National Security Letters Identified by the FBI

The OIG issued a report in March 2006 pursuant to Section 1001 of the Patriot Act, which included an evaluation of the FBI's process for reporting possible violations involving intelligence activities in the United

States to the IOB.[109] Among the types of possible IOB violations summarized in the report were instances in which the FBI may have improperly utilized national security letter authorities.[110]

In this section, we briefly summarize the FBI's procedures for reporting possible IOB violations to FBI-OGC and the manner in which FBI-OGC decides whether to report the possible violations to the IOB. We then describe the possible IOB violations regarding the use of national security letter authorities that were reported to FBI-OGC from 2003 through 2005; FBI-OGC's decisions whether to report the possible violations to the IOB; and other possible IOB violations involving national security letters that were not reported to FBI-OGC but that the OIG identified in the course of this review.

A. The IOB Process for Reporting Possible Violations of Intelligence Activities in the United States

Executive Order 12863 designates the IOB as a standing committee of the President's Foreign Intelligence Advisory Board and directs the IOB to inform the President of any 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.

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 possible IOB 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.

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

---

[109] See Office of the Inspector General, U.S. Department of Justice, *Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act* (March 8, 2006).

[110] The NSL-related possible IOB violations identified in the report occurred during Fiscal Years 2004 and 2005 and included incidents in which third parties provided e-mail content information that was not requested or authorized; an NSL that was issued after the investigation was extended without authorization; an NSL that was issued for the wrong subject with a similar name; and NSLs that were issued with typographical errors that led to the unauthorized collection information not relevant to an authorized national security investigation.

The first group 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 that the OIG identified during our review of a sample of 77 investigative files in the 4 field divisions we visited. We found that 17 files (22 percent) had one or more possible IOB violations. In total, the 17 files had 22 possible violations. To our knowledge, none of these 22 possible IOB violations was reported to FBI-OGC, and none was reported by FBI-OGC to the IOB.[111]

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

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. Table 6.1 summarizes these matters, followed by an additional description and our analysis.

---

[111] Of the 48 possible IOB violations in both categories, 28 occurred during preliminary investigations, 19 occurred during full investigations, and 1 occurred in the absence of a national security investigation. Thirty-two of the possible IOB violations occurred during counterterrorism investigations, 15 occurred during counterintelligence investigations, and 1occurred in the absence of a national security investigation.

TABLE 6.1

Summary of 26 Possible IOB Violations Triggered by Use of National Security Letters Reported to FBI-OGC (2003 through 2005)

Category of Possible IOB Violation	Number of Possible IOB Violations Reported to FBI-OGC		Number of Possible Violations Reported to the IOB
	FBI Error	Third Party Error	
Improper Authorization			
Issuing ECPA national security letter without obtaining required FBI Headquarters authorization to extend investigation after one year	1	0	1
Issuing ECPA national security letter without obtaining required SAC approval to initiate a national security investigation	1	0	1
Issuing RFPA national security letter without obtaining required approval to extend investigation	1	0	1
Improper Request Under Pertinent National Security Letter Statute			
Obtaining ECPA toll billing and RFPA financial records without first issuing national security letters	3	0	2
Issuing FCRA national security letter requesting consumer full credit report in a counterintelligence case	1	0	1
Unauthorized Collection			
Obtaining ECPA telephone subscriber information not relevant to an authorized national security investigation	2	0	1
Obtaining ECPA e-mail transactional information not relevant to an authorized national security investigation	1	3	4
Obtaining ECPA telephone toll billing records not relevant to an authorized national security investigation	12	1	8
Total FBI or Third Party Errors	**22**	**4**	
Total Possible IOB Violations	**26**		**19**

Nature of Possible IOB Violation and the NSL Statute at Issue: As noted in Table 6.1, these 26 possible IOB violations involved a variety of issues:

- In three matters, the NSLs were signed by the appropriate officials but the underlying investigations were not approved or extended by the appropriate Headquarters or field supervisors.
- In four matters, the NSLs did not satisfy the requirements of the pertinent national security letter statute or the applicable Attorney General Guidelines. In three of these matters, the FBI obtained the information without issuing national security letters. One of these three matters involved receipt of information when there was no open national security investigation. In the fourth matter, the FBI issued national security letters seeking consumer full credit reports in a counterintelligence investigation, which is not permitted by FCRAv.
- In 19 matters, 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.

Status of Investigative Subject and Target of NSL: FBI agents are required to include in their reports to FBI-OGC the status of the subject of the investigation as a "U.S. person" or a "non-U.S. person."[112] We also attempted to determine if the subject of the investigation in these 26 matters reported as possible IOB violations was the same as the target of the NSL.

- In 15 of the matters, the subject of the investigation was a "U.S. person," and in 8 of the matters the subject was a "non-U.S. person."[113]

---

[112] Section I(C)(1) of the NSI Guidelines, defines a "United States person" as:

a. an individual who is a United States citizen or alien lawfully admitted for permanent residence;

b. an unincorporated association substantially composed of individuals who are United States persons; or

c. a corporation incorporated in the United States.

[113] In one of the matters, the subject was a presumed "non-U.S. person," in one there was no subject, and in another the status of the subject could not be determined.

- In 19 of the matters, the NSLs sought information about the subject of the underlying national security investigation; 2 NSLs sought information on a target other than the snbject of the investigation; 1 NSL sought information on both the subject and a non-subject; 1 NSL was issued during a threat assessment (at which stage there is no subject); and 3 NSL targets could not be determined.

Source of the Error: In total, 22 of the 26 possible IOB violations were due to FBI errors, while 4 were due to third-party errors. The 22 possible IOB violations due to FBI error were:

- Receipt of financial records through use of FISA authorities rather than by issuing an RFPA NSL;
- Receipt of telephone toll billing records from a telephone company without first issuing an ECPA NSL;
- Eight NSLs containing typographical errors (seven on the telephonc numbers listed in the NSLs and one on the e-mail address listed in the NSL);
- Four NSLs concerning telephone numbers that responses to the NSLs revealed were no longer associated with the investigative subjects;
- An ECPA NSL requesting telephone toll billing records that was issued after the investigative authority had lapsed;
- Receipt of responses to two telephone toll billing record requests after the investigative authority had lapsed;
- A request for telephone toll billing records of an individual whose name was similar to that of the investigative subject;
- A request for financial records after the authority for the underlying investigation had lapsed;
- A request for telephone toll billing records during a criminal investigation before the Special Agent in Charge had approved conversion of the investigation to a counterterrorism investigation;
- Receipt of telephone toll billing records during a threat assessment through informal contact with FBI Headquarters Counterterrorism Division's Communications Analysis Unit; and
- A FCRA request for a consumer full credit report in a counterintelligence case.

The four third-party errors were:

- The NSL recipient providing prohibited content information (including facsimile images) in response to an ECPA NSL for telephone toll billing records; and
- The NSL recipient providing prohibited content information (including e-mail content and images) in response to three ECPA NSLs requesting electronic communication transactional records.

The following text box provides an example of a possible IOB violation.

Possible IOB Violation No. 1

In June 2004, during a file review of an authorized national security investigation of a foreign intelligence officer who was the target of a FISA court-authorized electronic surveillance order, a squad supervisor determined that a probationary case agent had on one occasion telephonically accessed the bank account of the investigative subject using information derived from the electronic surveillance order. The probationary agent had obtained the subject's bank account and personal identification number (PIN) to telephonically access the subject's bank account transactions and balance but did so without seeking approval to issue a national security letter for the records. The probationary agent had been assigned to a counterintelligence squad for 16 months at the time of the incident.

The squad supervisor told the probationary agent that the FBI was required to issue a national security letter under the RFPA before obtaining financial records in a foreign counterintelligence investigation. The agent indicated unfamiliarity with the statutory requirement. The agent was verbally counseled, and the squad supervisor promptly reported the matter to FBI-OGC as a possible IOB violation and to the FBI's Inspection Division and Office of Professional Responsibility. A RFPA national security letter later was issued to obtain the subject's financial records, including the information that was improperly obtained from FISA-derived information.

FBI-OGC determined that the matter should be reported to the IOB even if the agent was unaware that the agent was acting in contravention of the RFPA and internal FBI policy. The Inspection Division's Internal Investigations Section determined that the incident was indicative of a performance issue that did not warrant further investigation.

The following text box provides an example of the FBI's acquisition of telephone toll billing records in the absence of an active national security investigation.

Possible IOB Violation No. 2

In August 2005, a field division sent a lead to another field office concerning three suspicious telephone calls originating from the second division's jurisdiction. An intelligence analyst in the second division, under the supervision of a new Supervisory Analyst, requested via e-mail that the Counterterrorism Division's Communications Analysis Unit (CAU) "run" three numbers through its databases. CAU agreed to do so and also offered to obtain telephone toll billing records from a telephone company with the understanding that the requesting division would later prepare a national security letter to the telephone companies to cover the records obtained. The intelligence analyst agreed to the arrangement.

The same day, the intelligence analyst telephoned the Primary Relief Supervisor of a Resident Agency within the division regarding the lead on the suspicious calls. According to the field division's report to FBI-OGC, the intelligence analyst inferred that the telephone numbers were requested in the course of an ongoing substantive investigation by the first field division. The intelligence analyst requested that the Primary Relief Supervisor initiate the drafting of approval documents for the national security letter, but the intelligence analyst did not tell the Primary Relief Supervisor that he had already requested the records from CAU. About a week later, CAU sent the requested records to the intelligence analyst.

[redacted]

Because CAU had committed to the telephone company that it would furnish a national security letter after the fact to cover the records, the receiving division considered issuing a national security letter from its control file. However, the division's Chief Division Counsel, following consultation with the National Security Law Branch, determined that a national security letter could not be issued from its control file absent prior approval.

FBI-OGC concluded that the FBI's acquisition of the telephone toll billing records constituted a violation of the ECPA national security letter statute [redacted]

Reporting and Remedial Actions: Twenty of the 26 possible IOB violations were timely reported within 14 days of discovery to FBI-OGC in accordance with internal FBI policy. However, 6 were not reported in a timely fashion, taking between 15 days and 7 months to report.

We identified the remedial action that was taken regarding the 26 possible violations.

- In the 19 matters that involved unauthorized collection of information not relevant to an authorized national security investigation, field office documentation stated that the information was retrieved and segregated, reviewed no further, and sometimes forwarded to FBI-OGC for final disposition.[114] If the information had been uploaded or disseminated, FBI records showed that it was removed from the relevant databases and the disseminated information retrieved and segregated with the original information.
- In three of the matters that involved improper requests under pertinent national security letter statutes, field office documentation stated that the records received either were destroyed or sealed or that NSLs were issued for the requested records to cover the time period in question. In the fourth matter, one of the three NSLs was returned unexecuted when the FBI office that was to deliver the letter discovered the error and sent it back to the initiating office. Information from the NSL that had been disseminated to a foreign counterintelligence Task Force Officer was returned to the FBI without being used. The information inappropriately obtained from two NSLs was sealed and sent to FBI-OGC.
- In the three matters that involved improper authorization, field division documentation stated that the field division was instructed to cease further investigative activity in the investigation that was improperly extended without FBI headquarters authorization; an EC was sent to FBI Headquarters requesting approval to extend the investigation for six months; and the case agent submitted appropriate documentation to change the case designation to a counterterrorism case.

FBI-OGC decisions: FBI records show that FBI-OGC reported 19 of the 26 possible violations to the IOB. The FBI-OGC decided that the 7 remaining matters were not reportable to the IOB for the following reasons:

- In one of the matters, the FBI obtained telephone toll billing records on an investigative subject who was a "non-U.S. person" without issuing NSLs. The FBI-OGC decision stated that "only violations of the AG Guidelines which are designed to safeguard the rights of U.S. persons are required to be reported to the

---

[114] According to the CDC in one of the field offices we visited, case agents are advised to return telephone toll billing records it improperly acquires to the communication providers. If the providers do not want them back, the agents are advised to destroy the records and document the destruction with an Electronic Communication (EC). This field office did not usually send toll billing records to FBI-OGC for sequestration or destruction.

IOB."[115] The FBI-OGC decision memorandum noted that if the subject of the national security letter had been a "U.S. person" the matter would likely constitute a reportable IOB violation.

- In four matters, the FBI obtained telephone toll billing records or subscriber information that identified the telephone numbers with the investigative subjects. When the case agents reviewed the responses to the NSLs, they discovered that the telephone numbers were not associated with the investigative subjects. The FBI-OGC decisions stated that in each instance there was an authorized investigation for which NSLs were an appropriate investigative technique, and the NSLs were appropriately authorized. FBI-OGC also concluded that the case agents acted in good faith.
- In two related matters the FBI issued national security letters for telephone toll billing records during authorized national security investigations but the NSL recipient provided the results 35 days after expiration of the authority to conduct the investigation. The FBI-OGC decision stated that the FBI's receipt of the information did not constitute a violation of the Attorney General's NSI Guidelines because no investigative activity was conducted after the investigative authority had expired, and the case agent took appropriate steps to obtain approval to extend the investigation before conducting further investigative activity.

With regard to the FBI's decisions whether to report the possible violations to the IOB, we concurred in FBI-OGC's analysis and conclusions to report 19 of the 26 possible violations to the IOB. With one exception, we also concurred in its analysis and conclusions not to report the 7 remaining possible violations.

The one case in which 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 national security letters. 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

---

[115] According to internal FBI guidance, by longstanding agreement between the FBI and the IOB, E.O. 12334 has been interpreted to

> mandate the reporting of any violation of a provision of the foreign counterintelligence guidelines or other guidelines or regulations approved by the Attorney General, in accordance with E.O. 12333, if such provision was designed in full or in part to ensure the protection of the individual rights of a U.S. person.

to its internal administrative requirements was reportable "as a matter of policy" to the IOB. FBI-OGC's decision concluded that if the subject of the NSL had been a "U.S. person," this failure would "likely" constitute an IOB violation. Yet, we believe that FBI-OGC's rationale for not reporting the matter is inconsistent with at least four other possible IOB violations that were triggered by national security letters where the investigative subject or the target of the national security letter was a "non-U.S. person" but the matters were reported to the IOB.[116] We therefore disagree with FBI-OGC's determination that this matter should not be reported to the IOB.[117]

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

Our examination of the 26 possible IOB violations reported to FBI-OGC relating to the use of national security letters did not reveal deliberate or intentional violations of national security letter 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. While the errors resulted in the acquisition of information not relevant to an authorized investigation, they did not manifest deliberate attempts to circumvent statutory limitations or Departmental policies, and appropriate remedial action was taken.

However, we believe that three of the possible IOB violations arising from FBI errors were of a more serious nature because they demonstrated FBI agents' unfamiliarity with the constraints on national security letter authorities and inadequate supervision in the field. For example, in one instance, an FBI analyst was unaware of the statutory and internal FBI policy requirements that national security letters 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 national security letters – from information derived from FISA electronic surveillance orders. In these

---

[116] None of the FBI-OGC decision memoranda describing matters reported to the IOB involving non-U.S. Persons explained why these matters were reported to the IOB notwithstanding the status of the subject of the investigation or the NSL target.

[117] In November 2006, FBI-OGC issued guidance to all divisions for reports of possible IOB violations. The memorandum states that Section 2.4 of Executive Order 12863 has been interpreted to mandate the reporting of Attorney General Guidelines' violations "if such provision was designed to ensure the protection of individual rights." Accordingly, we do not believe that future decisions concerning whether to report possible IOB violations will be made solely on the basis of the non-U.S. person status of the investigative subject or the NSL target.

instances, it is clear that the agents and, in one instance, the squad supervisor, did not understand the legal constraints on the two types of national security letters or the interrelationship between FISA authorities and national security letter authorities.

II. Additional Possible IOB Violations Identified by the OIG During Our Field Visits

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 in our review of a sample of investigative files in the 4 field offices we visited. In those 77 investigative files, we reviewed 293 national security letters issued from 2003 through 2005. In those files, we identified 22 NSL-related possible IOB violations that arose in the course of 17 separate investigations, none of which 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.

A. Possible IOB Violations Identified by the OIG

Of the 22 possible IOB violations, 8 arose in eight investigations in Chicago, two arose in two investigations in New York, 8 arose in 4 investigations in Philadelphia, and 4 arose in three investigations in San Francisco. Seventeen occurred in counterterrorism investigations and 5 occurred in counterintelligence investigations. Thirteen possible IOB violations occurred during preliminary investigations, while 9 occurred during full investigations. The 22 possible IOB violations are summarized in Table 6.2.

TABLE 6.2

Summary of 22 Possible IOB Violations Triggered by Use of National Security Letters Identified by the OIG in Four Field Offices

Category of Possible IOB Violations	Number of Possible IOB Violations	
	FBI Error	Third Party Error
Improper Authorization		
Issuing national security letter without obtaining required approval to extend investigation	1	0
Improper Requests Under Pertinent National Security Letter Statute		
Issuing national security letter for material that arguably constituted prohibited content under ECPA	1	0
Issuing national security letter citing ECPA statute that requests RFPA financial records associated with e-mail accounts	1	0
Issuing national security letter for FCRAv consumer full credit report that included certification language either for RFPA financial records or FCRAu consumer or financial institution identifying information	3	0
Issuing national security letter requesting FCRAv consumer full credit report in a counterintelligence case	2	0
Issuing national security letter requesting FCRAv consumer full credit report when SAC approved national security letter for consumer identifying information or identity of financial institutions under FCRAu	4	0
Unauthorized Collection		
Obtaining information not relevant to an authorized national security investigation (subscriber information and telephone toll billing records)	0	4
Obtaining information beyond the time period requested in the national security letter (from 30 to 81 days in excess of request); obtaining consumer full credit report when SAC had approved NSL for limited credit information; obtaining toll billing records when NSL requested subscriber records	0	6
Total FBI or Third Party Errors	**12**	**10**
Total Possible IOB Violations	**22**	

We describe below the facts relating to these 22 matters, followed by our analysis of these possible violations.

Nature of Possible IOB Violation and NSL Statute at Issue: The 22 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 investigative authority had lapsed. As a result, under FBI policy and ECPA the NSL was sent in the absence of an authorized national security investigation.
- Nine NSLs involved improper requests under FCRAv, the newest NSL authority, which was established in the Patriot Act. Two of the 9 NSLs issued during one investigation requested consumer full credit reports during a counterintelligence investigation notwithstanding the fact that the statute authorizes consumer full credit report NSLs only in international terrorism investigations. Three of the 9 NSLs listed FCRAv as the authority for the request but the NSLs included the certification of relevance language either for the RFPA or the FCRAu NSL authority. In addition, 4 of these 9 NSLs were FCRA requests where the types of records approved by field supervisors differed from the records requested in the national security letters.
- 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 content arguably not permitted by the NSL statute.[118] The second NSL requested financial records associated with two e-mail addresses but requested the information under the ECPA rather than the RFPA, which 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 and electronic communication transactional records for longer periods than that specified in the NSL – periods ranging from 30 days to 81 days.[119] One NSL sought subscriber records pursuant to the

---

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

[119] We did not include in this category unauthorized collection of telephone toll billing records or subscriber information due to instances in which the communication provider furnished records beyond the time period specified in the NSL because of the communications provider's billing cycle.

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.

The following text box shows an example of agents' confusion regarding the two NSL authorities in the Fair Credit Reporting Act.

Possible IOB Violation No. 3

In October 2003, during a counterterrorism investigation, a field division counterterrorism squad obtained approval to issue a national security letter to a credit reporting agency seeking the names and addresses of all financial institutions at which the investigative subject, a "U.S. person," maintained accounts. The national security letter was issued pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681u(a), to determine the extent of the subject's financial holdings and to evaluate whether the subject provided material support to terrorist organizations.

In November 2003, a credit reporting agency provided a consumer full credit report on the investigative subject, instead of the more limited information the FBI had requested in the national security letter. Although the FBI was entitled to request a full consumer report if it established the necessary predicate under 15 U.S.C. § 1681v, this authority had not been approved by the Special Agent in Charge. Accordingly, even though the error was made by the credit reporting agency, the FBI's receipt of the additional information would be considered an unauthorized collection subject to reporting to FBI-OGC as a possible IOB violation. According to FBI records, the incident was not reported to FBI-OGC.

We found there was substantial confusion during the period covered by our review about how to address this and other matters related to the unauthorized acquisition of consumer full credit reports, including questions concerning (1) whether the FBI could use the full credit reports produced to the FBI even if they had not been requested; (2) whether agents should destroy the information, seal it, redact it, or ignore it; and (3) whether the matter should be reported to FBI-OGC as a possible IOB violation. The confusion was compounded by the decisions of two of the three major consumer credit bureaus to provide full consumer credit reports in response to all FBI FCRA national security letters, regardless of whether they requested only the limited information available under the original FCRA NSL statute. Ultimately, FBI-OGC decided that when the field agents receive full consumer credit reports in response to national security letters seeking more limited information, the agents should take the information the FBI is entitled to, seal the remainder, and file an IOB report. Following FBI-OGC meetings with credit bureau representatives in 2006, the two credit bureaus have agreed to redact information that is not requested in FBI NSLs.

Status of Investigative Subject and Target of NSL: Twelve subjects of the 17 investigations involving possible IOB violations identified by the OIG were "U.S. persons," 3 were "non-U.S persons," and two appeared to be "U.S. persons." In 18 of the matters, the NSLs sought information about the

subjects of the underlying investigations. In the remaining 4 matters, the NSL targets could not be determined.

Source of Error: 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.

Uploading of information obtained beyond time period specified in NSL request: We identified one instance in which the FBI uploaded into Telephone Applications from an NSL that exceeded the time period requested in the NSL. The NSL was issued during a full counterterrorism investigation of a U.S. person requesting toll billing records on the investigative subject's telephone number for the period September 1, 2002, to July 16, 2003. However, the FBI received and uploaded into its specialized application for telephone data telephone toll billing records information for two months in excess of the requested time period.

B. National Security Letter Issued in a Charlotte, N.C. Terrorism Investigation

In this section, we describe another possible IOB violation arising from the use of national security letter authorities that was not identified by the FBI. We learned of this possible violation through press accounts. For this reason we did not include it in the description of the results of our review of investigative files in the four field offices we visited. However, we believe this violation is noteworthy, and we therefore describe it in this section.

According to press accounts, the FBI's Charlotte Division was looking for information about a former student at North Carolina State University in connection with in the London subway and bus bombings in July 2005, who was later cleared of suspicion.[120] [redacted] The national security letter requested

[120] Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, The Washington Post, Nov. 6, 2005, at A1.

> Applications for admission, applications or statements concerning financial aid and/or financial situation, housing information, emergency contacts, association with any campus organizations, campus health records, and the names, without being redacted, of other students included in the records associated with the following information: . . . .

[redacted].

According to press accounts, university officials said that the FBI "tried to use a national security letter to demand much more information than the law allows." [redacted]. The university produced the records in response to a grand jury subpoena.

As discussed in Chapter Two, the ECPA NSL statute authorizes the FBI to obtain telephone toll billing records and subscriber information and electronic communication transactional records. It does not authorize the FBI to obtain educational records.[121] According to FBI records, the matter was not reported to FBI-OGC as a possible IOB violation. It also was not reported as a possible misconduct matter to the FBI's Office of Professional Responsibility.

---

[121] The production of educational records is governed by the Family Education Rights and Privacy Act of 1974 (FERPA), commonly referred to as "the Buckley Amendment." See 20 U.S.C. § 1232g. Generally, the Buckley Amendment prohibits the funding of an educational agency or institution that has a policy or practice of disclosing a student's records without parental or student consent if the student is over the age of 18. The law contains 16 exceptions to this general rule, one of which is known as the "law enforcement exception." In responding to a federal grand jury subpoena, the institution is not required to seek consent but must notify the parents and student in advance of compliance. See 20 U.S.C. § 1232g(b)(2)(B). However, for good cause shown, a court may order the institution not to disclose the existence of the subpoena or the institution's response. 20 U.S.C. § 1232g(b)(1)(J)(i).

C. OIG Analysis Regarding Possible IOB Violations Identified or Reviewed by the OIG

At the outset, it is significant to note that 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 IOB violations that the FBI identified in reports from all FBI Headquarters and field divisions for the same 3-year period (26). 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.

We have no reason to believe that the number of possible IOB violations we identified in the four field offices we visited was skewed or disproportionate to the number of possible IOB violations that exist in other offices. This suggests that a significant number of NSL-related possible IOB violations throughout the FBI have not been identified or reported by FBI personnel.

However, it is also significant to note that our review did not reveal intentional violations of the 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. For example, our interviews of 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.

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 which contained incorrect certifications or which sought records not referenced in the approval ECs. While the FBI was entitled to obtain the records sought and 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.

The reasons why the FBI did not identify the 23 possible IOB violations (counting the improper ECPA NSL involving the Charlotte Division) is unclear. Nine of the 23 matters were the types of possible violations that were self-reported by field divisions in the past, as noted in Section I above.[122] Thirteen of the remaining 14 matters involved discrepancies between the NSL approval ECs and the corresponding NSLs, the acquisition of records beyond the time period requested in the NSL, and the acquisition of a consumer full credit report and telephone toll billing records that were not requested by the NSLs. We believe that many of these infractions occurred because case agents and analysts do not carefully review the text of national security letters, do not consistently cross check the approval ECs with the text of proposed national security letters, and do not verify upon receipt that the information supplied by the NSL recipients 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 national security letter-related infractions that need to be reported to FBI-OGC as possible IOBs until November 2006. During our review, we noted frequent exchanges between Division Counsel and NSLB attorneys about what should and should not be reported as possible IOB violations involving NSLs which we believe showed significant confusion about the reporting requirements. However, the FBI did not issue comprehensive guidance about national security letter-related infractions until more than 5 years after the Patriot Act was enacted.[123] We believe the lack of guidance contributed to the high rate of unreported possible IOB violations involving national security letters that we found.

---

[122] These included issuing national security letters when the investigative authority had lapsed, issuing full credit report FCRA national security letters in a counterintelligence investigation, and unauthorized collections resulting from FBI typographical errors or third-party errors.

[123] The Inspection Division guidance dated February 10, 2005, generally described the revised procedures for reporting possible IOB violations. But this guidance did not address possible IOB violations that could arise from the FBI's expanded use of national security letters after the Patriot Act.

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

We identified two ways in which FBI Headquarters units in the Counterterrorism Division 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. In many instances there was no pending investigation associated with the request at the time the exigent letters were sent. In addition, while some witnesses told us that many 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 national security letters 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 by 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.

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

The Communications Exploitations Section (CXS) in the Counterterrorism Division at FBI Headquarters analyzes terrorist communications in support of the FBI's investigative and intelligence mission. One of the units in the CXS is the Communications Analysis Unit (CAU), established in approximately July 2002. The CAU's mission is to exploit terrorist communications and provide actionable intelligence to the Counterterrorism Division.

The CAU is designated an "operational support unit" rather than an operational unit. The consequence of this status is that under FBI internal policy the CAU cannot initiate counterterrorism investigations under the NSI Guidelines and cannot issue national security letters. NSLB attorneys told us that to the extent the CAU wants to obtain telephone toll billing records or other records under the ECPA NSL statute, the CAU has two options. One, it can ask the Headquarters Counterterrorism Division or an appropriate field division counterterrorism squad to issue a national security letter from an existing investigation to which the request was relevant. In those instances, as described in Chapter Three, in order to meet the NSI Guidelines' and ECPA standards, the CAU needs to generate approval memoranda articulating the relevance of the information sought to the pending investigation. Alternatively, if there is no pending investigation, the CAU can ask Headquarters operating units in the Counterterrorism Division or field office squads to: a) open a new counterterrorism investigation based on predication the CAU supplies that is sufficient to meet the NSI Guidelines and the ECPA, and b) issue a national security letter seeking information relevant to the new investigation.

As discussed in Chapter Three, only Special Agents in Charge of the FBI's field offices and specially delegated senior Headquarters officials are authorized to issue national security letters.

1. FBI Contracts With Three Telephone Companies

Following the September 11 attacks, the FBI's New York Division formed a group to assist in the analysis of telephone toll billing records that were needed for the criminal investigations of the 19 hijackers. A small group of agents and analysts assigned to examine the communication networks of the terrorists evolved into a domestic terrorism squad in the New York Division known as DT-6. During this time, the FBI's New York Division developed close working relationships with private sector companies, including telephone companies that furnished points of contact to facilitate the FBI's access to records held by these companies, including telephone records. The Supervisory Special Agent (SSA) who supervised DT-6 told us that he obtained Headquarters approval of and Headquarters financing for an arrangement whereby a telephone company representative would work with the New York Division to expedite the FBI's access to the telephone company's databases.

The SSA said that case agents on DT-6 generally provided grand jury subpoenas to the telephone company prior to obtaining telephone records. The grand jury subpoenas issued to the telephone company were signed by Assistant United States Attorneys who worked with FBI agents in the

criminal investigations growing out of the September 11 attacks.[124] However, in the period following the September 11 attacks, instead of initially sending a grand jury subpoena the case agents frequently furnished a "placeholder" to the telephone company in the form of a letter stating, in essence, that exigent circumstances supported the request. These "placeholder" letters – also referred to as "exigent letters" – were signed by SSAs or subordinate squad personnel.[125]

Between late 2001 and the spring of 2002, the value of the FBI's access to the telephone company prompted the FBI to enter into contracts with three telephone companies between May 2003 and March 2004. 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 the communications industry 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 CAU worked directly with telephone company representatives in connection with these contracts. Moreover, on the FBI's Intranet web site, CAU referenced its capacity to facilitate the acquisition of telephone records pursuant to the contracts. CAU presentations to counterterrorism squads in several field divisions also described the unit's capabilities, including its access to telephone company records. The slides used in CAU presentations referred to the CAU's ability to "provide dedicated personnel to service subpoenas/NSLs 24 x 7." In describing how the CAU should receive requests from the field, the slides noted that

> Field office prepares NSL or FGJS for CAU to serve on appropriate telecom provider.

---

[124] The SSA told us that an attorney with the telephone company established a tracking system to ensure that grand jury subpoenas were issued to cover all of the records obtained from the telephone company employees. The SSA also said that he checked regularly with a point of contact at the telephone company to determine if the FBI had fallen behind in providing legal process for these records. The SSA said he was confident that grand jury subpoenas were issued to cover every request.

[125] The SSA said that DT-6 case agents would sometimes provide the placeholder letters to the telephone company to initiate the search for records. The SSA said that in most instances by the time the records were available, a grand jury subpoena was ready to be served for the records.

-- Once paper received, CAU will obtain tolls/call details.

Thus, from this presentation, it appears that the CAU contemplated that the FBI would serve national security letters or grand jury subpoenas prior to obtaining telephone toll billing records and subscriber information pursuant to the three contracts, in conformity with the ECPA NSL statute.[126]

The Assistant Director of the Counterterrorism Division told us that based on numerous FBI briefings he received during his tenure, he directed his subordinates to contact the CXS Section Chief to ensure that the capabilities of the three companies were used. However, he also told us that he was unaware that any of the three companies were providing telephone toll billing records without first receiving duly authorized national security letters.

2. The Exigent Letters to Three Telephone Companies

The SSA who supervised DT-6 following the September 11 attacks told us that by late 2001 he and other DT-6 personnel were assigned to assist in the establishment of CAU at FBI Headquarters, and that they would have brought with them to Headquarters a copy of the exigent letter that had been used in the criminal investigations of the September 11 attacks to obtain information from the telephone company in New York. This letter was used by CAU personnel as a model to generate requests to the three telephone companies under contract with the FBI to provide telephone toll billing records or subscriber information. These exigent letters typically 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.

In response to our request, the FBI provided the OIG copies of 739 exigent letters addressed to the three telephone companies dated between March 11, 2003, and December 16, 2005, all but 4 of which were signed. The signed exigent letters included 3 signed by CXS Assistant Section Chiefs, 12 signed by CAU Unit Chiefs, 711 signed by CAU Supervisory Special Agents, 3 signed by CAU special agents, 2 signed by intelligence analysts, 1 signed by an intelligence operations specialist, and 3 that

[126] NSLB attorneys told us that NSLB attorneys were not consulted about the three contracts with the telephone companies or the procedures and administrative steps that CAU took following their implementation to obtain telephone toll billing records pursuant to the contracts. The FBI-OGC attorneys and a former CAU Unit Chief told us that to their knowledge the only OGC lawyers involved in reviewing the contracts were procurement lawyers.

contained signature blocks with no titles. Together, the 739 exigent letters requested information on approximately 3,000 different telephone numbers. The three highest volume exigent letters sought telephone toll billing or subscriber information on 117, 125, and 171 different telephone numbers.

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 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. Two CAU Unit Chiefs said they were confident that national security letters or grand jury subpoenas were ultimately issued to cover the FBI's receipt of information acquired in response to the exigent letters. The Unit Chiefs said that they relied on the telephone company representatives to maintain a log of the requests and to let CAU personnel know if any NSLs or grand jury subpoenas were needed. However, the Unit Chiefs acknowledged that because the CAU did not maintain a log to track whether national security letters or grand jury subpoenas were issued to cover the exigent letter requests and did not maintain signed copies of the exigent letters, they could not provide documentation to verify that national security letters or grand jury subpoenas were in fact issued to cover every exigent letter request.

Pursuant to administrative subpoenas, the OIG obtained from the three telephone companies copies of national security letters and grand jury subpoenas that the FBI served on the telephone companies in connection with FBI requests for telephone toll billing records or subscriber information from 2003 through 2005. The three telephone companies provided 474 national security letters and 458 grand jury subpoenas. However, CAU personnel told us that some of these NSLs and grand jury subpoenas were not related to the exigent letters and that CAU could not isolate which NSLs or grand jury subpoenas given to the OIG by the telephone companies were associated with the exigent letters. CAU officials told us that the only way the CAU could attempt to associate an exigent letter with a national security letter or grand jury subpoena was to query the ACS database system with the telephone numbers referenced in the exigent letters. Because the CAU officials stated that this would be a labor intensive exercise, we asked them to query ACS for the NSLs, grand jury subpoenas, or related documentation associated with 88 exigent letters that we randomly selected from the 739 exigent letters provided to us by the FBI.

The FBI provided the results of ACS queries for the first 25 of the 88 letters. To try to demonstrate that it issued either national security letters or grand jury subpoenas to cover the FBI's acquisition of the records obtained in response to the exigent letters, the FBI pointed to various

documents ranging from unsigned national security letters to e-mails referencing the telephone number listed in the exigent letters. Yet, the documents did not demonstrate that national security letters or grand jury subpoenas were issued to cover the records requested in the exigent letters. These documents included:

- Unsigned copies of 14 national security letters. The FBI provided approval ECs associated with only 8 of these 14 NSLs. Two of the NSLs were dated before the date of the corresponding exigent letters, three bore the same date as the corresponding exigent letters, and nine were dated after the date of the corresponding exigent letters. One of the unsigned NSLs was dated 481 days after the date of the corresponding exigent letter, and the rest were dated between 6 and 152 days after the corresponding exigent letters. Two unsigned NSLs were dated 10 and 13 days prior to the date of the corresponding exigent letters.
- Two ECs seeking approval to issue a national security letters, but no copies of the national security letters themselves.
- An e-mail dated 16 days prior to the date of the exigent letter asking CAU to "check" 7 telephone numbers, one of which was referenced in the exigent letter, and a note to the file indicating that the FBI had received records 10 days after the date of an exigent letter in response to a grand jury subpoena to 1 of the 3 telephone companies.[127]
- For the remaining eight exigent letters, documentation that did not reference directly or indirectly that national security letters had been issued relating to the records requested in the exigent letters.[128]

In sum, of the 88 exigent letters we randomly selected from the 739 exigent letters, the FBI produced unsigned national security letters for only 14 of the first 25 exigent letters. The documents provided for the first 25 exigent letters showed that the FBI would be unable to provide reliable documentation to substantiate that national security letters or other legal process was issued to cover the records obtained in response to many of the

---

[127] We cannot ascertain whether the subpoena was issued before or after the date of the "exigent letter."

[128] These documents included references to analyses of telephone data (5), an EC approving the closing of a preliminary investigation that was initiated after the date of the corresponding exigent letter (1), an EC documenting service of an NSL on a different telephone company than the one listed in the exigent letter (1); and an incomplete draft of an NSL requesting records listed in the corresponding exigent letter (1). We did not regard these to be reliable evidence that national security letters were issued in these instances for the records sought in the corresponding exigent letters.

exigent letters. Therefore, because of this clear finding in the first 25 letters and the labor intensive nature of the exercise, we did not ask the FBI to complete the sample of 88 letters.

3. Absence of Investigative Authority for the Exigent Letters

As discussed in Chapter Three, the national security letter statutes, the Attorney General's NSI Guidelines, and internal FBI policy require that Special Agents in Charge of field divisions or specially delegated Headquarters officials certify that the information sought in the national security letter is relevant to an authorized investigation. Since passage of the Patriot Act, the information requested in certain national security letters does not need to relate to the subject of the FBI's investigation, but can relate to other individuals as long as the information requested is relevant to an authorized national security investigation.

A former CAU Unit Chief told us that many of the exigent letters were generated in connection with significant Headquarters-based investigations as well as investigations in which the FBI provided assistance to foreign counterparts, such as investigations of the July 2005 London bombings. In some instances, CAU personnel said that the requests directed to CAU were communicated by senior Headquarters officials who characterized the requests as 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 were related to pending FBI investigations, and many exigent letters were not sent in exigent circumstances. As described in Chapter Three, these are required elements for NSL approval documentation necessary to establish compliance with the ECPA NSL statute, the NSI Guidelines, and internal FBI policy. Moreover, we learned from interviews of CAU personnel and FBI documents that when CAU requested telephone records from the three telephone companies pursuant to exigent letters, there sometimes were no open or pending national security investigations tied to the request.

We found that in the absence of a pending investigation CAU sent leads either to the Headquarters Counterterrorism Division (ITOS-1 or ITOS-2) or to field offices asking them to initiate new investigations from which the after-the-fact NSLs could be issued. However, CAU personnel told us that the 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.[129] When the field offices learned that the records had already been received, they complained to NSLB attorneys 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.

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 the three telephone companies without first issuing NSLs, CAU personnel circumvented the ECPA NSL statute and violated the NSI Guidelines and internal FBI policies. These matters 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 request could be tied, and failed to ensure that NSLs were issued promptly after the fact pursuant to existing or new counterterrorism investigations.

4. Efforts by the FBI's National Security Law Branch to Conform CAU's Practices to the Electronic Communications Privacy Act

NSLB attorneys responsible for providing guidance on the FBI's use of national security letter authorities told us that they were not aware of the 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 national security letter statute. Our review of contemporaneous e-mail commnnications and our interviews of CAU and NSLB personnel found that for nearly 2 years, beginning in late 2004, NSLB attorneys counseled CAU officials to take a variety of actions, including: 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 national security letters 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 national security letters could be issued in the absence of another pending investigation.[130] In addition, NSLB offered to dedicate personnel to

---

[129] 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.

[130] The Assistant General Counsel at first proposed the establishment of six "generic" or "umbrella" investigations files representing the recurring types of threats

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 June 2006, NSLB provided revised models for exigent letters to the Counterterrorism Division that stated that NSLs (rather than grand jury subpoenas) would be processed and served upon the telephone companies as expeditiously as possible. Pursuant to NSLB advice, the FBI continued to issue exigent letters since June 2006, using the new model letters.

As of March 2007, the FBI is unable to determine whether NSLs or grand jury subpoenas were issued to cover the exigent letters. However, at FBI-OGC's direction, CAU is attempting to determine if NSLs were issued to cover the information obtained in response to each of the exigent letters. If CAU is unable to document appropriate predication for the FBI's retention of information obtained in response to the exigent letters, the Deputy General Counsel of NSLB stated that the FBI will take steps to ensure that appropriate remedial action is taken. Remedial action may include purging of information from FBI databases and reports of possible IOB violations.

The Assistant General Counsel also told us that a different provision of ECPA could be considered in weighing the legality of the FBI's use of the exigent letters: the provision authorizing voluntary emergency disclosures of certain non-content customer communications or records (18 U.S.C. § 2702(c)(4)).[131] The Assistant General Counsel stated that while the FBI did

---

(cont'd.)

investigated by the Counterterrorism Division. The proposal contemplated that the FBI would issue national security letters from these files in exigent circumstances when there were no other pending investigations to which the request could be tied. After obtaining approval from NSLB supervisors to pursue this approach, the CAU Unit Chief told the NSLB Assistant General Counsel in September 2005 that generic national security investigations would not be needed because, contrary to his earlier statements, CAU would be able to connect each exigent letter request with an existing Headquarters or field division-initiated national security investigation. The Assistant General Counsel told us that she also was informed at this time by the CAU Unit Chief that the emergency requests were "few and far between."

[131] 18 U.S.C. § 2702 (c) provides:

Voluntary disclosure of customer communications or records.

* * *

(c) Exceptions for disclosure of customer records. – A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . .

* * *

(4) to a governmental entity, if the provider, in good faith, believes than an emergency involving danger or death or serious physical injury to any person

not rely upon this authority in issuing the exigent letters from 2003 through 2005, the FBI's practice may in part be justified by the ECPA's recognition that emergency disclosures may be warranted in high-risk situations. The Assistant General Counsel argued that in serving the exigent letters on the telephone companies the FBI did its best to reconcile its mission to prevent terrorist attacks with the strict requirements of the ECPA NSL statute.

The FBI General Counsel told us that the better practice in exigent circumstances is to provide the telephone companies letters seeking voluntary production pursuant to the emergency voluntary disclosure provision of 18 U.S.C. § 2702 (c)(4) and to follow up promptly with NSLs to document the basis for the request and capture statistics for reporting purposes. But the General Counsel said that, if challenged, the FBI could defend its past use of the exigent letters by relying on the ECPA voluntary emergency disclosure authority. The General Counsel also noted that the manner in which FBI personnel are required to generate documentation to issue NSLs can make it appear to an outsider that the records were requested without a pending investigation when in fact there is a pending investigation that is not referenced in the approval documentation due to the FBI's recordkeeping and administrative procedures.[132]

5. OIG Analysis of Exigent Letters

The FBI entered into contracts with three telephone companies in CY 2003 and CY 2004 for the purpose of obtaining quick responses to requests for telephone toll billing records and subscriber information. The documentation associated with the contracts indicated that the telephone companies expected to receive, and the FBI agreed to provide, national security letters or other legal process prior to obtaining the responsive records. Moreover, when the CAU described its mission to field personnel, it told them that the CAU expected to receive national security letters or other legal process before it obtained the records from the telephone companies. Neither the former Executive Assistant Director of the Counterterrorism and Counterintelligence Divisions nor any other Headquarters official told us that they approved the FBI's acquisition of records from the three telephone companies other than in response to duly authorized national security letters. Yet, the CAU issued over 700 exigent letters, rather than national

---

(cont'd.)

> requires disclosure without delay of information relating to the emergency; . . . .

[132] FBI-OGC attorneys told us that the FBI's acquisition of telephone toll billing records and subscriber information in response to the exigent letters has not been reported to the IOB as possible violations of law, Attorney General Guidelines, or internal FBI policy. We believe that under guidance in effect during the period covered by our review these matters should be reported as possible IOB violations.

security letters, to obtain telephone toll billing records information relating to over 3,000 different telephone numbers.

We found three additional problems with the CAU's exigent letters. First, each of the 739 exigent letters seeking telephone toll billing and subscriber records was signed by CAU Unit Chiefs and subordinate CAU personnel who were not authorized to issue national security letters under the ECPA and internal FBI policy. Second, when the CAU asked Headquarters or field divisions to issue national security letters after the fact in connection with existing investigations or to initiate new investigations from which the national security letters could be issued, the CAU generally did not inform other FBI employees that the records had already been obtained from the three telephone companies. Third, when the CAU asked Headquarters and field divisions to open new investigations out of which they could generate NSLs after the fact, CAU did not consistently provide information establishing predication for the request that was necessary to satisfy the ECPA NSL statute, the Attorney General's NSI Guidelines, and internal FBI policy.

We are not convinced by the legal justifications offered by FBI attorneys during this review for the FBI's acquisition of telephone toll billing records and subscriber information in response to the exigent letters without first issuing NSLs. The first justification offered was the need to reconcile the strict requirements of the ECPA NSL statute with the FBI's mission to prevent terrorist attacks. While the FBI's priority counterterrorism mission may require streamlined procedures to ensure the timely receipt of information in emergencies, the FBI needs to address the problem by expediting the issuance of national security letters or seeking legislative modification to the ECPA voluntary emergency disclosure provision for non-content records. Moreover, the FBI's justification for the exigent letters was undercut because they were (1) used, according to information conveyed to an NSLB Assistant General Counsel, mostly in non-emergency circumstances, (2) not followed in many instances within a reasonable time by the issuance of national security letters, and (3) not catalogued in a fashion that would enable FBI managers or anyone else to validate the justification for the practice or the predication required by the ECPA NSL statute.

We also disagree with the FBI's second justification: that use of the exigent letters could be defended as a use of ECPA's voluntary emergency disclosure authority for acquiring non-content information pursuant to 18 U.S.C. § 2702(c)(4). First, we found that the exigent letters did not request voluntary disclosure. The letters stated, "Due to exigent circumstances, it is requested that records . . . be provided" but added, "a subpoena requesting this information has been submitted to the United States Attorney's Office and "will be processed and served formally . . . as expeditiously as possible." In addition, we found that the emergency voluntary disclosure provision was

not relied upon by the CAU at the time, the letters were not signed by FBI officials who had authority to sign ECPA voluntary emergency disclosure letters, and the letters did not recite the factual predication necessary to invoke that authority.[133]

We also are troubled that the FBI issued exigent letters that contained factual misstatements. The exigent letters represented that "[s]ubpoenas 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." 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. Even if there were understandings with the three telephone companies that some form of legal process would later be provided to cover the records obtained in response to the exigent letters, the FBI made factual misstatements in its official letters to the telephone companies either as to the existence of an emergency justifying shortcuts around lawful procedures or with respect to steps the FBI supposedly had taken to secure lawful process.

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.

---

[133] Internal FBI guidance states that the only FBI officials authorized to sign voluntary emergency disclosure requests pursuant to 18 U.S.C. § 2702(c)(4) are Special Agents in Charge, Assistant Special Agents in Charge, Section Chiefs, or more senior officials.

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.

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

As discussed in Chapter Three, 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 national security letters may be used are national security investigations.

FBI internal policy also distinguishes between "investigative files" and "administrative files." Numerical codes are used to designate the FBI's various investigative programs, and other unique designations are used to establish non-investigative files, sometimes referred to as "control files" or "repository" files. The FBI's National Foreign Intelligence Program (NFIP) Manual states that investigative activity may not be conducted from control files, and that NSLs may only be issued in the course of national security investigations.[134]

However, we found that the FBI on occasion relied exclusively on "control files" rather than "investigative files" to initiate approval for the issuance of national security letters, in violation of internal FBI policy. Moreover, this practice made it difficult for FBI supervisors and others reviewing the proposed national security letters to determine if the required statutory predicate had been satisfied and whether the information sought was relevant to an authorized investigation in accordance with the NSI Guidelines.

1. National Security Letters Issued From a Headquarters Special Project Control File

During the first quarter of 2003, the FBI began to issue national security letters in connection with a classified special project. From 2003 through 2005, the CAU initiated NSL approval memoranda for approximately 300 national security letters in connection with this project, which were generated from a Headquarters control file. All of the resulting

---

[134] Section 19-03(L)(1) of the NFIP Manual states:

> [C]ontrol files are separate files established for the purpose of administering specific phases of an investigative matter or program and would not be considered a [preliminary investigation] or [full investigation.]

July 25, 2004.

NSLs sought telephone toll billing records, subscriber information, or electronic communication transactional records pursuant to the ECPA NSL statute. From the information available during the OIG review, it appears that all of the national security letters were served on the communications provider before any records were given to the FBI, and none of the information sought arose in emergency circumstances. The approval ECs for these NSLs do not refer to the case number of any specific pending FBI investigation.[135]

As noted above, CAU officials are not authorized to sign national security letters. A former CAU Unit Chief told us that, as a result, during the early phase of the project the CAU sent leads to field offices to initiate the process to issue these national security letters, but the CAU often met resistance. The Unit Chief said that some field offices responded diligently and pursued investigative activity to establish predication for opening a new counterterrorism investigation, while others did nothing.

To address the problem of issuing national security letters in the absence of timely field support, the CAU provided additional training to field personnel. In addition, the Unit Chief said that the Counterterrorism Division opened a special project control file from which the CAU sought approval from NSLB to issue national security letters for subscriber information. The CAU had used information in the control file to check indices to determine whether there was a nexus to terrorism that justified further investigative activity.

The classified nature of the project was such that few FBI Headquarters officials or OGC attorneys were authorized to know the predication for the NSL requests. This led to frustration and delays when field divisions were asked to respond to the CAU leads for the project. Because the CAU provided limited information about the predication for the leads to field offices, field-based counterterrorism squads sometimes opened threat assessments because they were not able to establish the required predication to open a national security investigation. In these instances, national security letters could not be issued in response to the CAU leads to field offices.

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.

---

[135] When we examined a sample of the approval ECs for these NSLs, we noted that some referred to telephone numbers or e-mail accounts believed to be associated with terrorist networks, while others stated that CAU had developed information from public and other sources identifying telephone numbers in contact with known terrorists.

2. National Security Letters Issued by the Electronic Surveillance Operations and Sharing Unit

The second circumstance we identified in the review in which national security letters were issued solely from control files related to leads sent by the Counterterrorism Division's Electronic Surveillance Operations and Sharing Unit (EOPS) in the CXS. EOPS' mission is to [redacted]. In 2003, EOPS opened a Headquarters control file to track its activities as well as the results of its analyses.[136]

An EOPS Unit Chief told us that EOPS initiated requests for national security letters in two circumstances. The first and most frequent circumstance was when field offices or Headquarters operational units requested EOPS' assistance in vetting subscriber information about some form of Internet usage. In these circumstances, the EC seeking approval for the national security letter would reference a "dual caption": the field or Headquarters division's investigative file number and the EOPS control file number. EOPS personnel told us that the FBI issued approximately 214 national security letters from 2003 through 2005 under "dual captions" that included an EOPS control file number.

The second and rarer circumstance occurred when, in the absence of a pending Headquarters or field-based national security investigation, EOPS sought approval for issuance of national security letters to verify subscriber or other information when EOPS alone developed the predication to support the request. These EOPS requests were prepared and forwarded for approval and issuance by the NSLB Deputy General Counsel. In these circumstances, EOPS assumed the role of "office of origin" for purposes of the request to NSLB. Documentation provided to us by the FBI indicated that the FBI sent six national security letters from 2003 through 2005 solely on the authority of control files.[137] The six NSLs sought information from Internet service providers. The requests for information initiated by EOPS were in the form of duly authorized national security letters prepared for the

---

[136] The Electronic Communication (EC) seeking approval to open this control file stated that its purpose was to "serve as a repository for communications concerning EOPS special projects, technical exploitation operations, and for tracking leads and taskings outside of EOPS operational case files." This type of approval EC would not reference investigative activity or facts supporting investigative activity. The subfile created in June 2005 from which the national security letters discussed in this section were issued also did not reference contemplated investigative activity.

[137] Three of the approval ECs referenced only an EOPS control file, while the three remaining approval ECs referenced an FBI legat office control file.

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. The database's limitations are discussed in Chapter Four and in the Classified Appendix.

signature of the NSLB Deputy General Counsel. The national security letters sought electronic communication transactional records, including the name, address, length of service, and billing records associated with specified e-mail addresses.

As discussed in Chapter Three, the approval EC accompanying an NSL request must document the predication for the national security letter by stating why the information is relevant to an authorized investigation. Yet, none of the six approval ECs accompanying the requests for these NSLs referred to the case number of any specific pending FBI investigation.[138]

A new EOPS Unit Chief recognized in August 2005 that the nature and quality of the work EOPS was generating out of the control file went beyond the conventional use of a control file. The EOPS Unit Chief began consulting with NSLB attorneys to make EOPS' "internal policies and procedures" conform to the FBI's national security letter practices. In December 2005, the Unit Chief sent an e-mail to an NSLB attorney acknowledging that EOPS was using a control file to seek Headquarters approval for the issuance of national security letters in response to numerous "hot projects," and that the Attorney General's NSI Guidelines require that a national security investigation be opened in order to issue national security letters. The Unit Chief noted that NSLB had approved using an EOPS repository or control file for certain unrelated purposes and asked if that control file could also be used for generating requests to issue national security letters.

The EOPS Unit Chief told us, however, that in his opinion EOPS was in compliance with FBI policy and the "spirit" of the Attorney General's Guidelines when it sought national security letters using EOPS as the "office of origin" because (1) the control file contained adequate information to support predication for a national security investigation; and (2) issuance of a national security letter did not constitute a "investigation" within the meaning of the Attorney General Guidelines. The Unit Chief noted that the NSLB Deputy General Counsel had been signing the national security letters, the predication was there, and it was "common sense" that issuing a national security letter was not a "full blown investigation." In the Unit Chief's view, so long as EOPS developed the requisite predication, the EOPS control file would serve as the investigation that would justify issuance of a national security letter because of the "uniqueness of the situation."

---

[138] Three of the six approval ECs sought issuance of ECPA NSLs regarding e-mail addresses identified as being used by a suspected terrorist. The remaining approval ECs sought records pertaining to an e-mail address identified as being associated with a terrorist group, an e-mail account that was in contact with e-mail accounts identified through FISA authorities, and an e-mail address that generated a threat to an intelligence community complaint center.

According to the Unit Chief, this would comply with the "spirit of the law," but not the letter of the law.

The NSLB Deputy General Counsel told us that in reviewing the documentation associated with national security letters generated by EOPS that she was asked to sign, she did not focus on the caption of the approval EC but rather on the factual recitation and whether the letter sought information on a "U.S. person" that impinged on First Amendment activity.[139] However, 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 and that, as of December 2006, she believes her advice has been followed.

3. OIG Analysis

According to the Attorney General's NSI Guidelines and the FBI's NFIP Manual, the issuance of a national security letter is an investigative technique that can be used only in connection with a national security investigation. Moreover, the national security letter statutes and the NSI Guidelines provide that national security letters may be issued only during authorized investigations. We believe that adherence to these three authorities requires that national security letters be issued from investigative files so that the requesting agent documents the existence of an authorized investigation and the relevance of the information sought to that investigation.

Although the distinction between a "control file" and an "investigative file" may seem obscure and technical, it is important for purposes of documenting compliance with the ECPA, the NSI Guidelines, and FBI policy. 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 the national security letters. 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 national security letter request can be tied or to have the connection described in the NSL approval EC. Control files are generally created for storing information that does not yet – and may never – satisfy the predicate for initiating a national security investigation. In our review, we found that approval ECs for the special project and EOPS NSLs did not

---

[139] The caption would have shown whether EOPS was requesting the national security letter exclusively out of its control file, out of an investigative file from Headquarters or a field division, or pursuant to a "dual caption" denoting more than one file.

provide documentation tying the requests to specific pending investigations or establishing the relevance of the information sought to pending investigations.

We believe that the CAU officials and the EOPS Unit Chief concluded in good faith that the FBI had sufficient predication either to connect these national security letters with existing investigations or to open new investigations in compliance with the Attorney General's NSI Guidelines. We also believe that the EOPS Unit Chief understood that national security letters should not be issued out of control files. We concluded, however, that issuing national security letters constitutes investigative activity, especially when the Attorney General's NSI Guidelines and the NFIP Manual plainly provide that national security letters are an "investigative technique" and that control files are not considered to be national security investigations.

In sum, we concluded that the Counterterrorism Division's use of control files rather than investigative files in connection with NSLs related to a classified special project and related to certain EOPS' activities, was contrary to internal FBI policy.

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

Our review also examined FBI investigative files to determine whether the field offices' use of national security letters violated FBI internal control policies. As discussed in Chapter Three, the FBI established procedures for the approval of national security letters to ensure that the requests contained sufficient information to allow field supervisors to confirm that the NSLs complied with applicable legal requirements and FBI policy. Periodic updates to the NFIP Manual and to the NSLB's Intranet web site also informed agents of the legal and internal policy requirements for each type of NSL. In addition, models, or "ponies," of approval electronic communications (ECs) and NSLs, which were available on the NSLB's Intranet web site, assisted case agents in completing the necessary paperwork to secure approval of national security letters.

The two key documents related to national security letters were the EC seeking approval to issue the NSL and the national security letter itself. According to FBI policy, each of these documents was required to reference information required either by the authorizing statutes or by FBI-OGC guidance.

In the sections below, we assess whether the national security letter documents we reviewed complied with these FBI policies. In addition, we discuss the violations of these policies that we found in our field office reviews of FBI investigative files.

1. Lapses in Internal Controls

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.[140]

We organized these infractions into three categories:

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 all of the required information; and

3) national security letters that did not contain the recitals or other information required by the authorizing statutes.

A large percentage of the investigative files we reviewed – 46 of 77, or 60 percent – contained one or more of these infractions. Nevertheless, in each of these cases, the national security letters were approved.

a. Failure to Document Review of NSL Approval Memoranda

The NFIP Manual and FBI-OGC guidance require that before a Special Agent in Charge signs a national security letter, the approval documents must be reviewed and initialed by the Supervisory Special Agent or Squad Leader, the Office of Chief Division Counsel, the Assistant Special Agent in Charge (ASAC), and the Special Agent in Charge.

Twenty-two of the 293 approval ECs (7 percent) we reviewed in eight different investigations did not reflect review or approval by these field supervisors or Division Counsel.[141] Seventeen of the 22 approval ECs with these infractions arose during counterterrorism investigations, while 5 arose during counterintelligence investigations. In five of the investigations, the subject of the investigation was a "U.S. person." In three cases, the subject of the investigation was a "non-U.S. person."

The elements missing from the 22 approval ECs were:

- 3 approval ECs did not reflect review and approval by the Special Agents in Charge;

---

[140] Based on our understanding of IOB reporting policies, these infractions did not rise to the level of possible IOB violations.

[141] Field personnel who are required to review NSLs are supposed to initial the approval EC. The approval ECs noted in this section did not contain the reviewer's initials, and we found no other documentation of approval in the investigative files.

- 18 approval ECs did not reflect review by the Assistant Special Agents in Charge (of which 15 were in a field division that suspended the requirement to route NSLs through the ASACs);
- 8 approval ECs did not reflect review by the Supervisory Special Agent; and
- 3 approval ECs did not reflect review by the Chief Division Counsel or Assistant Division Counsel.

b. Failure to Include Required Information in NSL Approval Memoranda

The NFIP Manual and FBI-OGC guidance require the approval EC to reference the statute authorizing the information requested; the status of the investigative subject as a "U.S. person" or "non-U.S. person"; the type and number of records requested; the predication for the request; leads showing transmittal of the approval EC to NSLB, the pertinent Headquarters operational division, and the squad or field division that was to deliver the national security letter; and the initialed approval of the request by the field supervisors and Chief Division Counsel.

We identified 99 of the 293 approval ECs (34 percent) we examined, in 40 different investigations, in which at least one of the four required elements was missing.[142] Thirty of the 40 files with these infractions were counterterrorism investigations, while 10 were counterintelligence investigations. In 31 instances, the investigative subject was a "U.S. person," in 8 instances, the investigative subject was a "non-U.S. person," and in one instance, the status of the investigative subject could not be determined.

The information missing from the 99 approval ECs was:

- 16 approval ECs did not reference the statute authorizing the FBI to obtain the information or cited the wrong statute;
- 66 approval ECs did not reference the "U.S. person" or "non-U.S. person" status of the investigative subject;
- 34 approval ECs did not specify the type and number of records requested; and
- 7 approval ECs did not recite the required predication for the request.

---

[142] We did not include in this category failures to include the required transmittals either to Headquarters operating divisions or field divisions for service. Sixty-six of the 293 approval ECs failed to include one or more of the required leads.

c. Failure to Include Required Information in National Security Letters

The NFIP Manual and FBI-OGC guidance require national security letters to reference the pertinent statutory authority, the type and number of records requested, the mandatory certification required by the referenced NSL statute, the non-disclosure provision, and the request that the provider deliver the records personally.[143]

We identified 5 of 293 national security letters (2 percent) we examined, in 3 different investigations that did not include at least one of these required elements. One of the infractions arose in a counterterrorism investigation, and four arose in counterintelligence investigations. In all three investigations, the investigative subject was a "U.S. person."

The five national security letters either did not include a reference to an NSL statute or referenced the wrong statute.

Finally, we note that 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 the 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.

2. OIG Analysis of Failures to Adhere to FBI Internal Control Policies

Complete and accurate documentation of the elements required for approval ECs and national security letters is essential to ensure compliance with the national security letter authorities, the Attorney General Guidelines, and internal FBI policy. If elements of the approval EC or the national security letter are missing, the FBI official signing the national security letter cannot be assured that the required predication, specifications of items sought, and statutory authority are correct.

We found significant numbers of NSL approval documents did not contain the required elements. The most notable elements missing (34 percent) occurred when field personnel failed to include the required information in NSL approval ECs. The absence of accurate information in these approval memoranda increases the risk of incorrect entries in the OGC database for tracking national security letters and may have produced incorrect reports to Congress with respect to the numbers of NSL requests and the status of investigative subjects.

---

[143] The absence of the Special Agent in Charge's signature on the national security letter would be considered a possible IOB violation and is not included in this category.

The instances in which field supervisors or Division Counsel failed to document their review of the NSL approval package, while few in number, were also serious. Review of the NSL package is designed to ensure that errors or inadequate predication are identified and corrected before a national security letter is issued.

Overall, we believe that the FBI has now provided needed guidance and support to field personnel to facilitate production of approval documentation compliant with statutory requirements, Attorney General Guidelines, and internal FBI policies. Nonetheless, we believe the FBI should improve its compliance with the internal controls governing the exercise of national security letter authorities by ensuring that its employees consistently and accurately satisfy all elements of the NSL approval documentation.

CHAPTER SEVEN
OTHER NOTEWORTHY FACTS AND CIRCUMSTANCES RELATED TO THE FBI'S USE OF NATIONAL SECURITY LETTERS

As directed by the Patriot Reauthorization Act, in this chapter our report includes other "noteworthy facts and circumstances" related to the FBI's use of national security letters that we found during our review. These matters include the interpretation of the Attorney General Guidelines' requirement to use the "least intrusive collection techniques feasible" with regard to the use of national security letters; uncertainty about the types of telephone toll billing records the FBI may obtain pursuant to an Electronic Communications Privacy Act (ECPA) national security letter; the review by Division Counsel of NSL requests; the issuance of NSLs from control files rather than investigative files, in violation of FBI policy; the FBI's use of "certificate letters" rather than Right to Financial Privacy Act (RFPA) national security letters to obtain records from Federal Reserve Banks; and the FBI's failure to include in its NSL tracking database the use of NSLs to obtain information about individuals who are not subjects of FBI investigations.

I. Using the "least intrusive collection techniques feasible"

When FBI agents evaluate the investigative techniques available to them at different stages of FBI investigations – including the use of national security letters – one of the factors they must consider is the intrusiveness of the technique. According to the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines), the intrusiveness of the investigative technique must be compared to the seriousness of the threat to national security that is being investigated and the strength of the information indicating such a threat. The NSI Guidelines, which were in effect for all but the first ten months of this review and remain in effect today, 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.[144]

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.[145]

For example, during our review, several senior FBI attorneys told us that legal precedents suggest that NSLs seeking telephone toll billing records and subscriber information do not implicate privacy interests under the Fourth Amendment. Several also said that they consider NSLs seeking financial records and consumer full credit reports to be more intrusive than NSLs seeking telephone toll billing records or subscriber information. However, the national security letter statutes and internal FBI policies do not address which of the national security letter authorities are more intrusive than others or the relative intrusiveness of NSLs compared to other investigative techniques.

These issues raise difficult questions that regularly arise regarding the FBI's use of national security letters. For example, under the NSI Guidelines, should case agents access NSL information about parties two or three steps removed from their subjects without determining if these contacts reveal suspicious connections? In light of the "least intrusive collection techniques feasible" proviso in the Attorney General Guidelines, is there 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? Are NSLs more or less intrusive than other investigative techniques authorized for use during national security investigations, such as physical surveillance? Yet, if agents are hindered from using all types of NSLs at early stages of 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 FBI Headquarters and field personnel we interviewed said that there is no uniform answer to the difficult question of how to use and sequence NSLs. Instead, they said that individualized decisions are made based on the evidence developed as the investigation proceeds. The FBI

---

[144] NSI Guidelines, § I(B)(2).

[145] OGC sent guidance on November 28, 2001, that referred to the "least intrusive" means proviso contained in the applicable FCI Guidelines. The guidance stated that

> supervisors should keep [the proviso] in mind when deciding whether or not a particular use of NSL authority is appropriate. The greater availability of NSLs does not mean that they should be used in every case.

General Counsel also expressed this view, stating that she believes that the use and sequencing of national security letters is best left to the experienced judgment of field supervisors. However, several Division Counsel told us that they believe it would be helpful if FBI-OGC's National Security Law Branch (NSLB) provided guidance on the interrelationship between the Attorney General's NSI Guidelines and the NSL statutes.

The impact of the FBI's investigative choices when using national security letters is magnified by three factors. First, as discussed in Chapter Four, 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 more clarity or at least a frame of reference.[146] 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 the appropriate use of these 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 FBI guidance as well as in the training of special agents, Chief Division Counsel, and all FBI officials authorized to sign NSLs.[147] With the FBI's increasing reliance on national security letters

---

[146] For example, the need for guidance was raised by a CDC in the context of considering whether it is appropriate to issue financial record and consumer full credit report NSLs in every terrorism investigation.

[147] One senior NSLB attorney told us that he does not believe that the training given to Special Agents in Charge adequately focuses on the use of NSL authorities, particularly in light of the volume of NSLs that field divisions are issuing. This attorney and other FBI Headquarters personnel told us that when NSLs are addressed at SAC training conferences, the focus is on the statutory requirements and internal FBI policies, such as the fact that SACs may not delegate authority to sign NSLs to Acting Special Agents in Charge or others.

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.

II. 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" pursuant to the ECPA NSL statute.

ECPA does not define the term "toll billing records information" and there is no case law interpreting the provision. Technological developments in the last twenty years also complicate what is meant by "toll billing records information." When the original ECPA NSL statute was enacted in 1986, most individuals had one landline telephone and were billed for each local and long distance telephone call. Now, many individuals have multiple cell phones or disposable cell phones, pre-paid phone cards, fixed rate phone plans, and text messaging capabilities.

In the absence of a statutory definition for "toll billing records information" 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.[148] For example, some telephone companies have told the FBI that while they maintain records of outgoing calls from a particular telephone number for business purposes, these records are not used for billing purposes and, thus, are not "toll billing records information." Other telephone companies provide long distance records but not records for local calls.

To assist case agents in ensuring that the FBI obtains the data permitted by the statute, FBI-OGC's National Security Law Branch has

---

(cont'd.)

However, SAC conferences have addressed a more intrusive investigative technique used in national security investigations. The FBI General Counsel told us that Special Agents in Charge were encouraged at a Senior Leadership Conference to terminate "full content" electronic surveillance pursuant to the Foreign Intelligence Surveillance Act if the technique is no longer productive, rather than continue to request authority to renew the surveillance orders over many years. Yet, there has been no comparable discussion of the use of NSL authorities.

[148] An Assistant General Counsel in NSLB told us that some telephone companies maintain records of individual calls made from a telephone number but do not bill for the calls. Instead, they "bundle" their services for a fixed fee. Some of these companies have told the FBI that they do not consider data retained for "unbilled calls" to be "toll billing records information."

developed sample attachments to NSLs for "toll billing records information" that list the types of records that the NSL recipient "may consider to be 'toll billing records information'." In June 2005, for example, NSLB posted sample attachments on its web site that referenced 12 categories of records, such as "local, regional, long distance, international, wholesale, cellular, paging, toll free, and prepaid calls." The attachment also contained the caveat that the FBI was not requesting, and the recipient should not provide, contents of any electronic communications.

However, 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."

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

FBI Division Counsel play a critical role in reviewing and approving national security letters. As discussed in Chapter Three, 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 any unauthorized information through any national security letters.

However, we believe that the timing of Division Counsel's review of NSLs and the supervisory structure for Division Counsel may affect the independence and aggressiveness of their review.

Division Counsel report to the Special Agents in Charge of the field offices in which they work, not to the Office of General Counsel at FBI Headquarters. As a result, personnel decisions such as performance reviews, compensation, and promotion determinations concerning Division Counsel are made by the Special Agents in Charge (SACs). We also found in our review that because Division Counsel report to SACs rather than to FBI-OGC, some Division Counsel are reluctant to question NSL requests or to challenge requests generated in the course of investigations that were previously approved by the SAC without CDC input.[149]

The tensions arising from the CDCs' reporting relationship with field managers were underscored by the results of an informal survey involving the use of NSL authorities. During our review, the CDC of a large field office reviewed an approval EC for an ECPA NSL that contained only one sentence

---

[149] CDCs are not required to review the documentation seeking approval to initiate national security investigations.

addressing predication for the request.[150] The CDC believed the NSL should not be approved, but was interested to know if his views were shared by CDCs in other field offices. To elicit their views, the CDC circulated the text of the request to 22 other CDCs, asking if they would have approved the NSL request. Responses to this informal survey revealed a split: 9 CDCs said they would approve the NSL request, while 13 said they would have rejected it.

The responses to the inquiry also generated much discussion as to whether there was sufficient predication for the request. For example, several CDCs said they would prefer to see more than a perfunctory statement that the investigation was authorized in accordance with the Attorney General Guidelines. Others disagreed, stating that so long as the approval EC recites the applicable legal standard, it is sufficient.

Apart from these legal disagreements as to whether the request satisfied the requirements of the ECPA statute, several CDCs said that they would have approved the request for reasons other than the merits of the approval documentation. After the inquiry, an Assistant General Counsel in NSLB (who would not have approved the NSL) spoke to some of the Division Counsel who said they would have approved the request. The Assistant General Counsel told the OIG that she learned that there were certain offices in which the CDC's relationship with the SAC was not "great," and where lawyers are viewed as trying to "stop things." The Assistant General Counsel said that she believed, after speaking to these attorneys, that some of the attorneys who said they would have approved the request would have preferred to reject it, but felt in a bind in challenging the SAC, particularly when the squad supervisor and Assistant Special Agent in Charge had already approved the underlying investigation. The Assistant General Counsel also said she thought several CDCs who would have approved the request did so "only to avoid the political fallout from questioning the initiation of a [national security investigation]."

As a result of the inquiry, FBI-OGC concluded that Division Counsel would benefit from more information in NSL approval documentation. Accordingly, in February 2006 OGC revised its guidance and standard formats for NSLs. Instead of requiring a "brief explanation" of the predication underlying the request, the ECs requesting approval to issue NSLs now are required to provide a "full explanation of the justification for

---

[150] The request stated:

> [An international terrorism] investigation of subject, a US PERSON, was authorized in accordance with the [Attorney General Guidelines] because the subject is in contact with the subjects of other international terrorism investigations. These subscriber and toll billing records are being requested to determine the identity of others with whom the subject communicates.

opening and maintaining the investigation on the subject" and to "fully state the relevance of the requested records to the investigation."

Another issue we found regarding the Division Counsel's review of national security letters was that, with exceptions in several of the FBI's largest field offices, Division Counsel do not learn about the underlying national security investigation until they are asked to review the NSL request. Therefore, the first time Division Counsel are likely to learn about the predication for national security investigations is when they see the first NSL in the investigations. As discussed above, until recently the documentation that case agents were required to prepare during the period covered by our review called for a "brief explanation" of the predication for the request. At times, agents merely recited the statutory language in the NSL approval memoranda.[151] Yet, some Division Counsel told us they are reluctant to second guess the predication for national security letters because they are unfamiliar with the underlying investigations – and, as noted above, are reluctant to second guess the operational judgments of senior field office officials. In fact, many CDCs said that the questions they raise with field personnel about the adequacy of predication for NSLs often results in contentious discussions with the requesting case agents and their supervisors.[152]

Finally, in considering the responses to the CDC's informal survey, the Assistant General Counsel and two NSLB Deputy General Counsel said they were very concerned that some CDCs believe they cannot exercise their independent professional judgment on the use of NSL authorities due to these concerns. We believe that, while the reporting structure for the Office of Chief Division Counsel raises questions that are beyond the scope of this review, they likely affect the CDC's role in approving the use of many other investigative authorities. We therefore recommend that the FBI consider measures to ensure that Chief Division Counsel and Assistant Division Counsel provide a hard review, and independent oversight, of NSL requests.

---

[151] NSLB posted the following guidance on its Intranet web site in March 2006 following passage of the Patriot Reauthorization Act:

> A perfunctory recitation that (1) the subject is the target of the investigation, (2) he has a telephone, and (3) therefore, it follows that an NSL for his telephone records is relevant to the authorized investigation will not suffice. Otherwise, any target with a telephone or a bank account is subject to an NSL. And that is not the standard for issuance of an NSL.

[152] One CDC who said he would not have approved the request stated that questions he has raised to explore the predication of NSLs and the relevance of the information sought to the investigations have caused more dissension in the office than any other issues he has encountered in over 20 years with the FBI.

IV. Issuing NSLs From "Control Files" Rather Than From "Investigative Files"

The Attorney General's NSI Guidelines and internal FBI policy authorize agents to initiate national security investigations when the required predication exists for a national security investigation. When these investigations are approved, the investigation is assigned a unique identifier that is referred to as the investigative file number. In contrast to these "investigative files," case agents may also seek approval to open "control files," sometimes referred to as "administrative files" or "repository files," which are created to store other types of FBI information. However, FBI policy does not permit investigative activity – such as issuing national security letters – to be conducted from a control file. Moreover, if a national security letter is issued from a control file, the NSL approval memorandum may not be accompanied by documentation explaining how the NSL request is tied to an existing national security investigation or the relevance of the information requested to that investigation.

As part of the FBI's post-September 11 reorganization, the Counterterrorism Division established several "operational support sections" that provide analytical support to counterterrorism investigations. As discussed in Chapter Six, we identified two circumstances in which over 300 national security letters were generated by Headquarters Counterterrorism Division personnel exclusively from "control files" rather than from investigative files.

FBI Headquarters officials, including Counterterrorism Division officials and NSLB attorneys, told us that the nature and quality of the work generated by these operational support units in coordination with other Headquarters and field divisions made these officials confident that there was sufficient predication for the NSLs issued exclusively from control files. However, these officials acknowledged that issuing NSLs exclusively from control files does not conform to internal FBI policy and makes it difficult to determine if the statutory and Attorney General's NSI Guidelines' requirements for issuing NSLs have been satisfied. We understand that the Counterterrorism Division, in consultation with FBI-OGC, has taken steps in response to the OIG's identification of this issue to ensure that future NSL requests are issued from investigative files rather than from control files so that these requests conform to NSL statutes, the Attorney General's NSI Guidelines, and internal FBI policy.

V. Obtaining Records From Federal Reserve Banks in Response to "Certificate Letters" Rather Than by Issuing RFPA NSLs

We identified instances in which the FBI sent at least 19 "certificate letters" to a Federal Reserve Bank seeking "financial records" concerning 244 named individuals instead of issuing NSLs pursuant to the Right to

Financial Privacy Act (RFPA).[153] Most of the individuals whose records were sought were subjects of FBI investigations, but some were other individuals. The certificate letters were issued between May 2003 and August 2004 and were signed by a Unit Chief in the Headquarters Counterterrorism Division's Terrorist Financing Operations Section (TFOS), a TFOS Acting Unit Chief, or Supervisory Special Agents assigned to TFOS. While the letters did not consistently specify what type of "financial records" were sought, TFOS officials told us that the FBI obtained "Fedwire records" in response to the letters.[154] Although the letters were issued at least 18 months after passage of the Patriot Act, they recited the pre-Patriot Act legal standard for acquiring the records.[155] The FBI General Counsel and other FBI-OGC attorneys told us that they were not aware that the FBI had obtained records from a Federal Reserve Bank without first issuing RFPA NSLs.

NSLB attorneys first learned of the certificate letters in July 2004, when a TFOS Acting Assistant Section Chief told an NSLB Assistant General Counsel that the certificate letters merely asked the Federal Reserve Bank whether it had information on the referenced bank account and that TFOS obtained the records themselves only after they served RFPA NSLs. TFOS personnel also told the Assistant General Counsel that the letters were used with few exceptions only in emergency situations, and that NSLs or grand jury subpoenas were issued relatively soon after the records were provided to the FBI to cover the records obtained in response to the certificate letters. While some TFOS personnel told the Assistant General Counsel that Federal Reserve Bank employees who dealt with TFOS did not believe NSLs were required in order for the FBI to obtain the records because the Federal Reserve Banks were "quasi-governmental bodies," the Assistant General Counsel believed at the time that NSLs were required before the FBI could obtain the records. The Assistant General Counsel instructed TFOS in August 2004 that any requests for information from Federal Reserve Banks be reviewed to ensure that they do not seek financial records in the initial requests and that such requests should omit the reference to the RFPA NSL statute.

Contrary to the statements made to the Assistant General Counsel by TFOS personnel noted above, the Assistant General Counsel discovered by

---

[153] The FBI did not retain signed copies of the certificate letters and, therefore, Counterterrorism Division personnel could not confirm the total number of the letters.

[154] Fedwire is the Federal Reserve's electronic funds and securities transfer service. Banks and other depository institutions use Fedwire "to move balances to correspondent banks and to send funds to other institutions on behalf of customers." See www.newyorkfed.org.

[155] The letters contained certifications that there were "specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power as defined in 50 U.S.C. § 1801."

accident in the fall of 2004 that the certificate letters requested the records themselves, not just that a search be conducted. The Assistant General Counsel also learned that the certificate letters were often used in non-emergency situations; and there were delays as long as six months in issuing NSLs after obtaining the information. Following these discoveries, in December 2004 the Assistant General Counsel again counseled TFOS to revise the certificate letters to ask that only a search be conducted and that the FBI should only obtain the records after issuing duly authorized NSLs except in genuine emergencies.

The Assistant General Counsel also met with attorneys in the Federal Reserve's Office of the General Connsel (OGC) who said that the Federal Reserve's position on whether to require NSLs depended on who the FBI's point of contact was at the Federal Reserve. The Assistant General Counsel told us that the issue was resolved when Federal Reserve OGC attorneys told the Assistant General Counsel that the Federal Reserve considered itself to be a "financial institution" and therefore would require NSLs before releasing financial records under the RFPA.

Prior to the conclusion of this review, the OIG contacted Federal Reserve Bank attorneys who stated that they believe Federal Reserve Banks are not "financial institutions" for purposes of the RFPA NSL statute and that Fedwire records are not "financial records" under the statute. Nonetheless, the Federal Reserve OGC attorneys said that Federal Reserve Banks as a matter of policy require that the FBI issue RFPA NSLs before the FBI may obtain Fedwire records and "financial records." After reviewing the certificate letters, these attorneys also stated that the Federal Reserve Banks should not have provided Fedwire records in response to the certificate letters because the certificate letters are not duly authorized RFPA NSLs.

The OIG also asked FBI-OGC and the OIG General Counsel for their legal opinion as to whether Federal Reserve Banks are "financial institutions" for purposes of the RFPA NSL statute and whether Fedwire records are "financial records" under the statute. Although we do not reach a definitive conclusion in this review, we cannot conclude that the FBI's practice of issuing certificate letters signed by subordinate TFOS personnel violated the RFPA.

We also note our concern about (1) the ability of NSLB attorneys in FBI-OGC to obtain accurate and complete information about the FBI's use of NSL authorities; and (2) the delay in TFOS' compliance with NSLB's advice. TFOS personnel provided inaccurate information to the Assistant General Counsel who inquired about TFOS' practice of issuing certificate letters rather than NSLs and failed to ensure that the initial advice given to TFOS was promptly communicated and implemented. As a consequence of the inaccurate information conveyed to NSLB and the delay in implementing

NSLB's advice, the FBI issued at least three additional certificate letters to a Federal Reserve Bank in contravention of NSLB's legal advice.

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

As discussed in Chapter Three, since passage of the Patriot Act the standard for issuing national security letters has changed and the FBI no longer needs to identify individualized suspicions about the targets of the NSLs. Instead, the FBI is authorized to collect information on any individuals so long as the information is relevant to an authorized investigation and, with respect to investigations of "U.S. persons," the investigations are not conducted solely on the basis of activities protected by the First Amendment. Thus, the target of an NSL is frequently not the same person as the subject of the underlying investigation. For example, if the response to an NSL for toll billing records on the subject's telephone number identifies a telephone number that the subject contacted frequently during a time period relevant to the investigation, the FBI may issue another NSL requesting subscriber information for that telephone number.

As described in Chapter Four, for purposes of preparing the congressional reports on NSL usage, the FBI-OGC NSL tracking database (OGC database) captures the numbers of investigations of different U.S. Persons and non-U.S. persons that generated NSL requests. However, the OGC database does not capture data on whether the target of the NSL is the subject of the underlying investigation 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.

Our review assessed this issue in the sample of investigative files we examined in four field offices. Of the 293 national security letters we examined, we identified 13 instances (4 percent) in which the NSLs requested information on individuals other than the investigative subjects.

We also found that during the period of our review, FBI-OGC did not consistently require case agents to include in the memoranda seeking approval to issue NSLs whether the NSL target was the subject of the underlying investigation. In 2006, the FBI modified its guidance to require, with the exception of NSLs seeking subscriber information, that agents indicate in the 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.

We believe the FBI should also modify the FBI database to include data, which is contained in the approval ECs, reflecting the number of NSL

requests for information on U.S. persons and non-U.S. persons who are not the investigative subjects but are the targets of NSLs. 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.

CHAPTER EIGHT
CONCLUSIONS AND RECOMMENDATIONS

As required by the Patriot Reauthorization Act, this OIG review examined the FBI's use of national security letters from calendar years 2003 through 2005. The Act required the OIG to examine how many requests were issued by the FBI; any noteworthy facts or circumstances relating to such use, including any improper or illegal use of such authority; the importance of the information acquired to the intelligence activities of the Department of Justice or to others; the manner in which such information is collected, retained, analyzed, and disseminated by the Department; whether and how often the Department utilized such information to produce an analytical intelligence product for distribution within the Department of Justice, to the intelligence community, or to others; and whether and how often the Department provided such information to law enforcement authorities for use in criminal proceedings.

Our review found that the FBI's use of national security letter requests 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.

When considering these statistics, it is important to note that one national security letter may contain more than one request for information. For example, the 39,000 NSL requests in 2003 were contained in approximately 12,000 letters, and the 47,000 requests in 2005 were contained in approximately 19,000 letters.

Most NSL usage (about 74 percent of all NSL requests) 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.

National security letters seeking telephone toll billing records or subscriber information or electronic communication (e-mail) transactional records or subscriber information accounted for the overwhelming majority of NSL requests during the review period ([redacted] percent), [redacted] ([redacted] percent) and [redacted] ([redacted] percent).

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 numbers of NSLs and NSL requests issued by the FBI are significantly higher than the FBI reported.

Further, we found the OGC database did not accurately reflect the status of investigative subjects or other targets of NSLs 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 classification of those individuals' status 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 national security letters 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 investigations, or enable agents to close investigations; providing investigative leads; and corroborating information obtained by 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. When prosecutors review FBI investigative files, they also may see information obtained through national security letters. 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 also determined that information obtained from national security letters is routinely stored in the FBI's Automated Case Support (ACS) system; Telephone Applications, a specialized FBI application for storing telephone data; the FBI's Investigative Data Warehouse database; 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.

As required by the Patriot Reauthorization Act, our review also examined instances of improper or illegal use of national security letters. First, our review examined national security letter violations that the FBI was required to report to the President's Intelligence Oversight Board (IOB). Executive Order 12863 directs the IOB to inform the President of any activities that the IOB believes "may be unlawful or contrary to Executive order or presidential directive." The FBI identified 26 possible violations involving the use of national security letter authorities from 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, including records containing data beyond the time period requested in the national security letters. 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 possible violations relating to national security letters that were not identified by the FBI. These possible 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 possible violations (22 percent), we believe that a significant number of NSL-related possible 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 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 matters 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 exclusively 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 Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, 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 establish 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 does not retain copies of signed 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 describes several other "noteworthy facts or circumstances" we identified. 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 who 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 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 requirements of the ECPA NSL statute when it issued at least 739 "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 a counterintelligence investigation, and when it sought and obtained financial records and telephone toll billing records without first issuing NSLs.

Based on our review, we believe that the FBI should consider the following recommendations relating to the use of national security letters. 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 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. Consider issuing 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. As directed by the Patriot Reauthorization Act, the OIG will examine the FBI's use of national security letter authorities and report on their use in calendar year 2006.

UNCLASSIFIED

APPENDIX

The Attorney General
Washington, D.C.

March 1, 2007

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

Dear Mr. Fine:

I appreciate your work and the opportunity to comment on your Review of the Federal Bureau of Investigation's Use of National Security Letters.

The problems identified in your review are serious and must be addressed immediately. I have spoken with FBI Director Bob Mueller about your findings and recommendations. He already has taken specific steps to correct past mistakes and to ensure that the Bureau will use National Security Letters (NSLs) in an appropriate manner in compliance with all applicable laws and internal policy requirements.

I have asked the Department's National Security Division and the Privacy and Civil Liberties Office to work with the Bureau in implementing these corrective actions and to consider any further review and reforms that are needed. They will report to me regularly on their progress. In addition, I ask that you report to me in four months on the FBI's implementation of your recommendations.

Your review also evaluated the effectiveness of NSLs and rightly found them to have "contributed significantly to many counterterrorism and counterintelligence investigations." NSLs are vital investigative tools and are critical to our efforts to fight and win the war on terror. They can and must be used appropriately and in a manner that protects the civil liberties of all Americans. I have confidence in the Director's ability to implement the changes necessary to ensure the proper use of these authorities.

Sincerely,

Alberto R. Gonzales

UNCLASSIFIED
DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

E/S 00145

MEMORANDUM FOR: Glenn A. Fine
Inspector General
Department of Justice

SUBJECT: (U) Department of Justice Office of the Inspector General's Draft Report: "A Review of the Federal Bureau of Investigation's Use of National Security Letters"

(U) Thank you for requesting my comments, pursuant to Section 119(d) of the USA PATRIOT Improvement and Reauthorization Act of 2005, on the Department of Justice (DOJ) Office of the Inspector General's Draft Report entitled "A Review of the Federal Bureau of Investigation's Use of National Security Letters" (Report).

(U) I appreciate your efforts, and the efforts of your staff, in producing an in-depth Report on this important issue. I have significant concerns about the issues raised in the Report. I anticipate that many of the recommendations contained in the Report will be implemented in order to ensure that the Federal Bureau of Investigation (FBI) has improved processes and procedures to ensure full compliance with all laws and regulations in its use of National Security Letters (NSLs). To ensure that the FBI's changes are successful, and that the FBI's use of NSLs is consistent with the U.S. Constitution, statutes, Executive Orders, and regulations, I directed the General Counsel and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence to work with DOJ and the FBI to remedy deficiencies identified in your final report, as appropriate.

(U) My highest priority is protecting America while ensuring that all activities undertaken to protect our citizens by the Intelligence Community fully comply with all laws. While not lessening my concern about the issues identified in the Report, I think it is important to note that NSLs are critical tools in counterterrorism and other investigations. As your Report notes, information obtained from NSLs "contributed significantly to many counterterrorism and counterintelligence investigations." Many of these details on sensitive investigative matters must remain classified, but your Report contains important examples where NSLs have provided critical information to protect America. Indeed, as your Report notes, FBI personnel believe NSLs are "indispensable investigative tools." Of course, as with all investigative tools, it is vital that NSLs are used in a manner that complies with all applicable laws and regulations.

(U) Thank you again for your efforts.

J M McConnell
J. M. McConnell

28 FEB 07
Date

UNCLASSIFIED

U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535-0001

March 6, 2007

Honorable Glenn A. Fine
Inspector General
United States Department of Justice
Suite 4706
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

SUBJECT: U.S. Department of Justice, Office of the Inspector General - "**A Review of the Federal Bureau of Investigation's Use of National Security Letters (NSL).**"

Dear Mr. Fine:

The FBI appreciates this opportunity to respond to findings and recommendations made in your report entitled "A Review of the Federal Bureau of Investigation's Use of National Security Letters" (hereinafter "Report"). This letter conveys the FBI's responses to the recommendations, and I request that it be appended to the Report. The Office of the Inspector General (OIG) has identified areas of serious concern related to the FBI's use of National Security Letters (NSLs). The FBI has already taken several steps to correct the deficiencies identified in the Report. These steps are described in more detail below and include strengthening internal controls, changing policies and procedures to improve oversight of the NSL approval process, barring certain practices identified in the Report, and ordering an expedited inspection. We will continue to work with the OIG to gauge our progress in these reforms.

Before addressing the specific findings and recommendations in the Report, the FBI offers two general comments applicable to the FBI's use of this critical national security investigative tool. First, I appreciate the OIG's discussion in the Report of the importance of National Security Letters to our counterterrorism and intelligence missions. When Congress expanded the FBI's ability to use this vital tool, some expressed concern about a potential for abuse. It is important to note that the OIG found no intentional or deliberate misuse of these authorities but highlighted several areas where we must increase our internal audit and oversight of these tools. We are doing so, and we will work in concert with the Department's National Security Division and Privacy and Civil Liberties Office to implement these reforms.

As the Report notes, NSLs are indispensable investigative tools that permit the FBI to gather the basic building blocks in national security investigations, enabling the FBI both to advance such investigations and, when warranted, to close such inquiries with a higher degree of confidence that the subject does not pose a terrorism threat. On page 46 of the Report and in the ensuing pages, the Report catalogues 8 vital functions NSLs play in the FBI's mission to protect the American people. For instance, the Report cites examples where NSLs helped enable investigators to establish potential contacts of an investigative subject and to determine whether a terror cell may be operating in a particular location. As the Report notes, these are the types of "bread and butter" capabilities FBI Agents rely on to advance national security investigations.

With these functions in mind, I deeply appreciate the OIG's observation that any discussion of the FBI's use of National Security Letters must take into consideration the environment in which the FBI -- particularly the Counterterrorism Division (CTD) -- has functioned for the last five years. Since September 11, 2001, the FBI has transformed its operations while working at a breakneck pace to keep the country safe. As the OIG noted, the FBI has "overhaul[ed] its counterterrorism operations, expand[ed] its intelligence capabilities, [begun] to upgrade its information technology systems, and [sought] to improve coordination with state and local law enforcement agencies." It is important to note that during the period reviewed, CTD was investigating and responding to a constant stream of terror threats. For instance, the investigation into the Al Qaeda plot that culminated in the attacks of September 11 was still ongoing in 2003 when CTD began investigating potential plots to destroy U.S.-bound aircraft and individuals surveilling economic targets in the United States. The 2005 bombings in London prompted intensive investigations of any known U.S. connections. These high-profile investigations occurred at the same time as CTD was conducting literally hundreds of lower profile investigations.

I believe those first two points -- the extraordinary workload of CTD since September 11 and the importance of National Security Letters to our national security efforts -- are critical to remember when considering the OIG's congressionally mandated assessment of "improper or illegal" use of national security letter authorities. I am pleased that the OIG found no criminal use of these authorities nor any deliberate or intentional violations of the national security letter statutes or the Attorney General Guidelines. Nevertheless, I conclude from the OIG's findings that we must redouble our efforts to ensure that there is no repetition of mistakes of the past in the use of these authorities, however lacking in willfulness was the intent. To that end, it is worth noting that the FBI considers all reports of possible violations of its legal authorities seriously and requires regular reporting, legal review, and referrals to the appropriate entities. If unauthorized information is obtained, whether due to FBI or third-party error, that information is sealed, sequestered, and where appropriate, destroyed. In addition, employee conduct is reviewed and disciplined appropriately.

As the Report makes clear, in the majority of cases, the desire of Agents to expedite the conduct of national security investigations for the protection of the American public resulted in the FBI obtaining information to which it was entitled. While well-intentioned, the shortcuts identified by the OIG were unacceptable. Because they may have been facilitated in part by unclear internal guidance, we have already published improved internal guidance and have prohibited certain practices that the OIG criticized. We are also developing a comprehensive training module to address any uncertainty that exists within our employee ranks about the legal strictures that govern the use of National Security Letters. That training will be mandatory for Special Agents in Charge (SAC), Chief Division Counsels (CDC), and counterterrorism and counterintelligence Agents. Finally, because the vast majority of the uses of NSLs that the OIG flagged as improper originated with the CTD, I ordered an expedited, special inspection of that area of responsibility within CTD and the practices identified by the OIG.

Second, prior to commencement of the IG review, the FBI had identified deficiencies in our system for generating the data necessary for required congressional reporting of NSL usage. Those deficiencies, which were first flagged for Congress in March 28, 2006, resulted in errors in the numbers reported to Congress. We appreciate the OIG identifying additional deficiencies that we had not noted in the way we track and report usage of NSLs. Independent of this report, we have made substantial progress in developing an automated system to prepare NSLs and their associated documentation, which will automatically gather data for congressional reporting. This system, which will be described in more detail below, should alleviate many of the concerns identified by the FBI and the OIG. Other deficiencies identified by the OIG have already been corrected for future reporting purposes.

Recommendations:

OIG's recommendations below outline important and necessary controls when issuing National Security Letters and maintaining corresponding (statistical) records.

Recommendation #1: Require all Headquarters and field personnel who are authorized to issue National Security Letters to create a control file for the purpose of retaining signed copies of all National Security Letters they issue.

The FBI agrees with the OIG recommendation that the FBI should retain a signed copy of the National Security Letter and is implementing a policy that would require the originating office to maintain a copy of the signed NSL in the investigative sub-folder of the

authorized investigation to which the NSL is relevant. The FBI believes that maintaining the NSL copy with the corresponding investigative file is more appropriate than creating a control file for this purpose.

Recommendation #2: Improve the FBI-Office of General Counsel (OGC) NSL tracking database to ensure that it captures timely, complete, and accurate information on NSLs and NSL requests.

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

The FBI agrees with these OIG recommendations. In fact, the FBI began addressing this issue in February 2006, when contractors produced an initial proposal for an automated system to prepare and track National Security Letters. This system is intended to be built as part of the existing, highly succeessful FISA Management System (FISAMs). For the last year, the FBI, with the assistance of its contractors, has been in the process of designing a database that is referred to as the NSL sub-system of FISAMs. The NSL sub-system is scheduled for testing in the Washington Field Office in July 2007, with the expansion of the system to other field offices pending successful testing.

The NSL sub-system is designed to require the user to enter certain data before the workflow can proceed and requires specific reviews and approvals before the request for the NSL can proceed. Through this process, the FBI can automatically ensure that certain legal and administrative requirements are met and that required reporting data is accurately collected. For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system will be able to verify the status of that file to ensure that it is still open and current (e.g., request date is within six months of the opening or an extension has been filed for the investigation) and ensure that NSLs are not being requested out of control or administrative files. The system will require the user to separately identify the target of the investigative file and the person whose records are being obtained through the requested NSL, if different. This will allow the FBI to accurately count the number of different persons about whom we gather data through NSLs. The system will also require that specific data elements be entered before the process can continue, such as requiring that the target's status as a U.S. person (USPER) or non-U.S. person (NON-USPER) be entered.

The NSL sub-system is being designed so that the FBI employee requesting an NSL will enter data only once. The system will then generate both the NSL and the authorizing Electronic Communication (EC) for signature, thereby ensuring that the two documents match exactly and minimizing the opportunity for transcription errors that give rise to unauthorized

collections that must be reported to the Intelligence Oversight Board (IOB). As with the FISA Management System, this subsystem will have a comprehensive reporting capability.

With regard to other deficiencies indicated in your report that affect the accuracy of our congressional reporting, the default settings in our existing "database" have been changed: the default position for the U.S. person status of the "target" of the NSL has been changed to U.S. person and "0" can no longer be entered for the number of facilities on which data is requested by an NSL.

Recommendation #4: Consider issuing 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.

The FBI agrees with the OIG recommendation. As indicated above, the NSL subsystem is anticipated to reduce if not eliminate typographical errors that result in unauthorized collection of information. OGC issued comprehensive advice on November 11, 2006, with respect to reporting unauthorized collection of all types and provided guidance with respect to the sequestration of such materials. OGC will issue additional comprehensive NSL guidance that will, among other things, highlight the legal differences between the two NSL authorities that appear in the Fair Credit Reporting Act. Given the finding of the IG of at least two instances in which an NSL was issued under 15 U.S.C. § 1681v in counterintelligence investigations, we are directing each field office to inspect its counterintelligence files to determine whether it has made the same mistake. If any additional instances of that error are found, appropriate remedial action, including reports to the Intelligence Oversight Board, will be taken. The FBI does not believe that the issuance of National Security Letters from control files is legally improper if, as was the case, the NSLs sought information that was relevant to authorized national security investigations that were open at the time the NSLs were issued. The FBI recognizes, however, that referring solely to a control file in the EC that seeks issuance of the NSL does not adequately document the existence of a national security investigation to which the material sought is relevant. Therefore, we are reiterating existing FBI policy that National Security Letters should be issued exclusively from investigative files and that such investigative files should be referenced on the supporting EC. Finally, although many of the possible IOB violations identified by the IG do not rise to the level of violations that are required to be reported to the IOB, the field has been instructed to report all to OGC for further evaluation.

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

The FBI agrees with the OIG recommendation. The FBI agrees with the OIG's recommendation to seek a clarification of statutory definition of "telephone toll billing records information."

Recommendation #6: Consider measures that would enable FBI Agents and analysts to (a) label or tag their use of information derived from National Security Letters and (b) identify when and how often information derived from NSLs is provided to law enforcement authorities for use in criminal proceedings.

FBI agrees with the OIG recommendation, I have asked OGC to work with the FBI's National Security Branch and the Office of the Director of National Intelligence to ensure we carefully consider this recommendation balancing our operational needs, information sharing policy, and privacy concerns.

Recommendation #7: Take steps to ensure that the FBI does not improperly use exigent letters.

Recommendation #8: Take steps to ensure that where appropriate the FBI makes requests for information in accordance with the requirements of National Security Letter authorities.

The FBI agrees with the OIG recommendations. It is important to note that an "exigent" letter as that term is used in the Report is not an emergency disclosure under 18 U.S.C. 2702 (c) but rather a letter asking for records from a service provider upon the promise of a forthcoming NSL or grand jury subpoena. The "exigent letter" discussed in the Report never sought the content of any communications. While the FBI does not believe that the use of exigent letters is improper in itself, it recognizes that they have been used improperly as noted in the Report. Therefore, as a matter of policy, the FBI has barred their use.

Recommendation #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 through the use of National Security Letter authorities.

The FBI agrees with the OIG recommendation. As part of the OGC's issuance of comprehensive guidance on National Security Letters, it will implement a more rigorous approval process to include the following: (1) for National Security Letters issued by Field Offices, the EC supporting the National Security Letter must be reviewed and approved by the Chief Division Counsel or Assistant Division Counsel (ADC); and (2) for National Security

Honorable Glenn A. Fine

Letters issued by Headquarters, the EC must be reviewed and approved by the National Security Law Branch of the Office of General Counsel.

Recommendation #10: Ensure that Chief Division Counsel and Assistant Division Counsel provide close and independent review of requests to issue National Security Letters.

The FBI agrees with the OIG recommendation. The FBI has taken steps to address this issue already. In February 2006, the Office of the General Counsel, National Security Law Branch, reminded all Chief Division Counsels of the importance of their role in the National Security Letter approval process. In March 2006, the National Security Law Branch included on its website a narrative description of the role of the CDCs and the ADCs in approving National Security Letters. Additionally, the FBI General Counsel has reminded all Special Agents in Charge that their office's CDCs have an obligation to provide accurate, independent legal advice and that the SACs should strive to encourage such independent advice from the CDCs. Finally, the General Counsel will stress to the CDCs during the next regularly scheduled teleconference the importance of their exercising independent legal judgment in all FBI matters, including those surrounding the NSL process.

The FBI is committed to protecting the people of the United States in a manner consistent with its statutory authority, guidelines, and policy. I appreciate this opportunity to respond to your recommendations and will update you and the appropriate congressional committees with regard to our implementation progress.

Sincerely yours,

Robert S. Mueller, III
Director

NATIONAL SECURITY LETTER STATUTES IN EFFECT PRIOR TO USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005

Right to Financial Privacy Act

12 U.S.C. § 3414

(a)(1) Nothing in this chapter (except sections 3415, 3417, 3418, and 3421 of this title) shall apply to the production and disclosure of financial records pursuant to requests from--

(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities;

(B) the Secret Service for the purpose of conducting its protective functions (18 U.S.C. 3056; 3 U.S.C. 202, Public Law 90-331, as amended); or

(C) a Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

(3) No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that a Government authority described in paragraph (1) has sought or obtained access to a customer's financial records.

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director) certifies in writing to the financial institution that such records are sought for foreign counter intelligence purposes 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.

(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(C) On the dates provided in section 415b of Title 50, the Attorney General shall fully inform the congressional intelligence committees (as defined in section 401a of Title 50) concerning all requests made pursuant to this paragraph.

(D) No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under this paragraph.

(b)(1) Nothing in this chapter shall prohibit a Government authority from obtaining financial records from a financial institution if the Government authority determines that delay in obtaining access to such records would create imminent danger of--

(A) physical injury to any person;

(B) serious property damage; or

(C) flight to avoid prosecution.

(2) In the instances specified in paragraph (1), the Government shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

(3) Within five days of obtaining access to financial records under this subsection, the Government authority shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the Government authority setting forth the grounds for the emergency access. The Government authority shall thereafter comply with the notice provisions of section 3409(c) of this title.

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(d) For purposes of this section, and sections 3415 and 3417 of this title insofar as they relate to the operation of this section, the term "financial institution" has the same meaning as in subsections (a)(2) and (c)(1) of section 5312 of Title 31, except that, for purposes of this section, such term shall include only such a financial institution any part of which is located inside any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the United States Virgin Islands.

Fair Credit Reporting Act
Financial Institution and Consumer Identifying Information

15 U.S.C. § 1681u

(a) Identity of financial institutions

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 3401 of Title 12) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that such information 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.

(b) Identifying information

Notwithstanding the provisions of section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information 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.

(c) Court order for disclosure of consumer reports

Notwithstanding section 1681b of this title or any other provision of this subchapter, if requested in writing by the Director of the Federal Bureau of Investigation, or a designee of the Director in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, a court may issue an order ex parte directing a consumer reporting agency to furnish a consumer report to the Federal Bureau of Investigation, upon a showing in camera that the consumer report 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.

The terms of an order issued under this subsection shall not disclose that the order is issued for purposes of a counterintelligence investigation.

(d) Confidentiality

No consumer reporting agency or officer, employee, or agent of a consumer reporting agency shall disclose to any person, other than those officers, employees, or agents of a consumer reporting agency necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation under this section, that the Federal Bureau of Investigation has sought or obtained the identity of financial institutions or a consumer report respecting any consumer under subsection (a), (b), or (c) of this section, and no consumer reporting agency or officer, employee, or agent of a consumer reporting agency shall include in any consumer report any information that would indicate that the Federal Bureau of Investigation has sought or obtained such information or a consumer report.

(e) Payment of fees

The Federal Bureau of Investigation shall, subject to the availability of appropriations, pay to the consumer reporting agency assembling or providing report or information in accordance with procedures established under this section a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching, reproducing, or transporting books, papers, records, or other data required or requested to be produced under this section.

(f) Limit on dissemination

The Federal Bureau of Investigation may not disseminate information obtained pursuant to this section outside of the Federal Bureau of Investigation, except to other Federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation, or, where the information concerns a person subject to the Uniform Code of Military Justice, to appropriate investigative authorities within the military department concerned as may be necessary for the conduct of a joint foreign counterintelligence investigation.

(g) Rules of construction

Nothing in this section shall be construed to prohibit information from being furnished by the Federal Bureau of Investigation pursuant to a subpoena or court order, in connection with a judicial or administrative proceeding to enforce the provisions of this subchapter. Nothing in this section shall be construed to authorize or permit the withholding of information from the Congress.

(h) Reports to Congress

(1) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on Banking, Finance and Urban Affairs of the House of Representatives, and the Select Committee on Intelligence and the Committee on Banking, Housing, and Urban Affairs of the Senate concerning all requests made pursuant to subsections (a), (b), and (c) of this section.

(2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 415b of Title 50.

(i) Damages

Any agency or department of the United States obtaining or disclosing any consumer reports, records, or information contained therein in violation of this section is liable to the consumer to whom such consumer reports, records, or information relate in an amount equal to the sum of-

(1) $100, without regard to the volume of consumer reports, records, or information involved;

(2) any actual damages sustained by the consumer as a result of the disclosure;

(3) if the violation is found to have been willful or intentional, such punitive damages as a court may allow; and

(4) in the case of any successful action to enforce liability under this subsection, the costs of the action, together with reasonable attorney fees, as determined by the court.

(j) Disciplinary actions for violations

If a court determines that any agency or department of the United States has violated any provision of this section and the court finds that the circumstances surrounding the violation raise questions of whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee who was responsible for the violation.

(k) Good-faith exception

Notwithstanding any other provision of this subchapter, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or identifying information pursuant to this subsection in good-faith reliance upon a certification of the Federal Bureau of Investigation pursuant to provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(l) Limitation of remedies

Notwithstanding any other provision of this subchapter, the remedies and sanctions set forth in this section shall be the only judicial remedies and sanctions for violation of this section.

(m) Injunctive relief

In addition to any other remedy contained in this section, injunctive relief shall be available to require compliance with the procedures of this section. In the event of any successful action under this subsection, costs together with reasonable attorney fees, as determined by the court, may be recovered.

Fair Credit Reporting Act
Consumer Full Credit Report

15 U.S.C. § 1681v

(a) Disclosure

Notwithstanding section 1681b of this title or any other provision of this subchapter, a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file to a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism when presented with a written certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.

(b) Form of certification

The certification described in subsection (a) of this section shall be signed by a supervisory official designated by the head of a Federal agency or an officer of a Federal agency whose appointment to office is required to be made by the President, by and with the advice and consent of the Senate.

(c) Confidentiality

No consumer reporting agency, or officer, employee, or agent of such consumer reporting agency, shall disclose to any person, or specify in any consumer report, that a government agency has sought or obtained access to information under subsection (a) of this section.

(d) Rule of construction

Nothing in section 1681u of this title shall be construed to limit the authority of the Director of the Federal Bureau of Investigation under this section.

(e) Safe harbor

Notwithstanding any other provision of this subchapter, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a government agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

Electronic Communications Privacy Act

18 U.S.C. § 2709

(a) Duty to provide.--A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification.--The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may--

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation 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; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made 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 upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of certain disclosure.--No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) Dissemination by bureau.--The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) Requirement that certain congressional bodies be informed.--On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

National Security Act

50 U.S.C. § 436

(a) Generally

(1) Any authorized investigative agency may request from any financial agency, financial institution, or holding company, or from any consumer reporting agency, such financial records, other financial information, and consumer reports as may be necessary in order to conduct any authorized law enforcement investigation, counterintelligence inquiry, or security determination. Any authorized investigative agency may also request records maintained by any commercial entity within the United States pertaining to travel by an employee in the executive branch of Government outside the United States.

(2) Requests may be made under this section where--

(A) the records sought pertain to a person who is or was an employee in the executive branch of Government required by the President in an Executive order or regulation, as a condition of access to classified information, to provide consent, during a background investigation and for such time as access to the information is maintained, and for a period of not more than three years thereafter, permitting access to financial records, other financial information, consumer reports, and travel records; and

(B)(i) there are reasonable grounds to believe, based on credible information, that the person is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(ii) information the employing agency deems credible indicates the person has incurred excessive indebtedness or has acquired a level of affluence which cannot be explained by other information known to the agency; or

(iii) circumstances indicate the person had the capability and opportunity to disclose classified information which is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Each such request--

(A) shall be accompanied by a written certification signed by the department or agency head or deputy department or agency head concerned, or by a senior official designated for this purpose by the department or agency head concerned (whose rank shall be no lower than Assistant Secretary or Assistant Director), and shall certify that--

(i) the person concerned is or was an employee within the meaning of paragraph (2)(A);

(ii) the request is being made pursuant to an authorized inquiry or investigation and is authorized under this section; and

(iii) the records or information to be reviewed are records or information which the employee has previously agreed to make available to the authorized investigative agency for review;

(B) shall contain a copy of the agreement referred to in subparagraph (A)(iii);

(C) shall identify specifically or by category the records or information to be reviewed; and

(D) shall inform the recipient of the request of the prohibition described in subsection (b) of this section.

(b) Disclosure of requests

Notwithstanding any other provision of law, no governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person, other than those officers, employees, or agents of such entity necessary to satisfy a request made under this section, that such entity has received or satisfied a request made by an authorized investigative agency under this section.

(c) Records or information; inspection or copying

(1) Notwithstanding any other provision of law (other than section 6103 of Title 26), an entity receiving a request for records or information under subsection (a) of this section shall, if the request satisfies the requirements of this section, make available such records or information within 30 days for inspection or copying, as may be appropriate, by the agency requesting such records or information.

(2) Any entity (including any officer, employee, or agent thereof) that discloses records or information for inspection or copying pursuant to this section in good faith reliance upon the certifications made by an agency pursuant to this section shall not be liable for any such disclosure to any person under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(d) Reimbursement of costs

Any agency requesting records or information under this section may, subject to the availability of appropriations, reimburse a private entity for any cost reasonably incurred by such entity in responding to such request, including the cost of identifying, reproducing, or transporting records or other data.

(e) Dissemination of records or information received

An agency receiving records or information pursuant to a request under this section may disseminate the records or information obtained pursuant to such request outside the agency only--

(1) to the agency employing the employee who is the subject of the records or information;

(2) to the Department of Justice for law enforcement or counterintelligence purposes; or

(3) with respect to dissemination to an agency of the United States, if such information is clearly relevant to the authorized responsibilities of such agency.

(f) Construction of section

Nothing in this section may be construed to affect the authority of an investigative agency to obtain information pursuant to the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.) or the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

Mr. CONYERS. Thank you, Attorney General.

Will the person in the back row, standing up, please sit down or leave this Committee room?

I am now pleased to welcome the General Counsel for the Federal Bureau of Investigation, Ms. Valerie Caproni.

Welcome to our Committee.

TESTIMONY OF VALERIE CAPRONI, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION

Ms. CAPRONI. Thank you. Good morning.

Mr. Chairman, Ranking Member Smith and Members of the Committee, it is my pleasure to appear before you today to discuss the recent report by the Department of Justice Office of Inspector General regarding the FBI's use of National Security Letters. I have submitted a detailed written statement, and in the interest of time, I will stress only a few points.

The IG's report is a fair report that acknowledges the importance of National Security Letters to the ability of the FBI to keep the country safe and the difficult environment in which our employees have been working since 9/11. The IG found no deliberate or intentional misuse of the National Security Letter authorities, AG guidelines or FBI policy. Nevertheless, the IG review identified several areas of inadequate auditing and oversight of these vital investigative tools as well as processes that were simply inappropriate.

The FBI fully supports each of the IG's recommendations and have implemented other remedial steps not proposed by the IG. Collectively, these reforms will ensure full compliance with both the letter and the spirit of the law.

NSLs generally permit us to obtain the basic building blocks of an investigation from third party businesses. Unlike grand jury subpoenas used in criminal cases, however, National Security Letter authority comes from several distinct statutes, and they have very specific rules that accompany them.

The NSL authority used most frequently by the FBI is that provided by the Electronic Communications Privacy Act, or ECPA. Through an ECPA NSL, the FBI can obtain subscriber information for telephone and electronic communications and can obtain toll billing information and electronic communication transaction records. Significantly, the FBI cannot obtain the content of communications through an ECPA NSL. That requires a court order. ECPA NSLs are, by far, the most common NSL that we use.

Pursuant to the Right to Financial Privacy Act and the Fair Credit Reporting Act, we also have the authority to issue different types of National Security Letters. The authority to issue an NSL lies at a senior level within the FBI. It can only be issued by an official who ranks not lower than Special Agent in Charge or Deputy Assistant Director. All such officials are career Government employees, and before an NSL can be issued such employees must certify that the information sought is relevant to an authorized national security investigation.

As directed by Congress in connection with the IG's report, we endeavor to declassify as much information as possible in order to maximize the transparency of our use of this important national security tool. To that end, for the first time the public has a real

sense of the frequency with which the FBI uses National Security Letters. In the period covered by the report, the number of NSL requests—that is, not letters. Remember that one letter can have multiple requests—has ranged from approximately 40,000 to 60,000 per year, and we have requested information on fewer than 20,000 persons per year. For a variety of reasons that will be discussed below, those numbers are not exact. Nevertheless, for the first time, the public can get a sense of the order of magnitude of these requests.

There are three findings by the IG that were particularly disturbing to me, and it is those three findings that I wish to address at some length this morning: First, inaccurate reporting to Congress, second, the use of so-called Exigent Letters and, third, violations of law and policy with respect to the usage of NSLs.

I am particularly distressed by the fact that the IG found significant inaccuracies in the numbers that we report to Congress. The responsibility to gather the data for congressional reporting lies with my division, and we did not do an acceptable job. The processes we put in place for tabulating NSLs were inadequate, and we had no auditing process in place to catch errors. Although we realized we had a problem prior to the IG's report and were working on a technological solution, that realization came later than it should have, and for that I bear responsibility.

At some point several years before I arrived at the FBI, our process for congressional reporting shifted from a totally manual process to a stand-alone database. While the OGC database was a giant technological step forward from 3x5 index cards, it quickly became an unacceptable system given the increase in our use of National Security Letters since 9/11. The OGC database is not electronically connected to ACS, the system from which we derive the data. Instead, there is a manual interface between ACS and the database. An OGC employee is responsible for taking every NSL lead that is sent to OGC and manually entering the information into our database. Nearly a dozen fields must be manually entered, including the file number of the case in which the NSL was issued, which is typically at least 15 digits and letters. Needless to say, human error creeps in.

Approximately a year ago when we were unable to tick and tie numbers in the database to previously reported numbers, we recognized that our technology was woefully inadequate. We began at that point to develop an automated system to improve our ability to collect this data. That system, in addition to improving data collection, will automatically prevent many of the errors in NSLs that we will discuss today by automating much of the work associated with preparing NSLs. The system will also allow us to automatically ensure that required reporting data is accurately collected. The NSL system is being designed so that the FBI employee requesting an NSL will enter data only once.

For example, an agent or an analyst who wishes to get telephone toll billing records will only have to tell the system that he is seeking an ECPA NSL for toll records and type the telephone number once. The system will then automatically populate the appropriate fields in the NSL in the authorizing electronic communication. The system will ensure that the two documents match exactly, and it

will minimize the opportunity for transcription errors that gave rise to unauthorized collections.

Agents and analysts will still be required to provide the narrative necessary to explain why the NSL is being sought, the factual basis for making the determination that the information is relevant to an appropriately predicated national security investigation and the factual basis for any determination that the NSL should include a nondisclosure provision.

We are optimistic that we will be able to pilot the system this summer and roll it out to all of the field offices by the end of the year. At that point, I will be much more confident that in the future the data we provide to Congress is as accurate as humanly possible. In the meantime, we are taking several steps to correct the numbers we have previously reported. We have discussed our methodology with the IG, and we will offer him the opportunity to review our work. We are striving to have the corrected reports to Congress as soon as possible.

The next significant finding of the IG I would like to discuss this morning involves the use within one unit at headquarters of so-called Exigent Letters. These letters, which numbered in excess of 700, were provided to telephone companies with requests for toll billing information. All of the letters stated that there were exigent circumstances, and many stated the Federal grand jury subpoenas had been requested for the records even though in fact no such requests for grand jury subpoenas had been made.

From an audit and an internal control perspective, the FBI did not document the nature of the emergency circumstances, did not keep copies of all of the Exigent Letters it provided to the telephone companies and did not keep records to track whether it had subsequently provided further legal process. Moreover, some employees told the IG that there was not always an emergency relating to the documents that were sought.

OGC has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record that we have in an FBI database was obtained because it was relevant to an authorized investigation and that the appropriate legal process has now been provided. If we are unable to determine the investigation to which a number relates, it will be removed from our database, and the records will be destroyed.

The IG rightfully objected to the FBI's obtaining telephone records with a letter that stated that a Federal grand jury subpoena had been requested when that was untrue. It is unclear why that happened. The Director has ordered a special inspection in order to better understand the full scope of internal control failures and to make sure that, in fact, every record obtained pursuant to a so-called Exigent Letter has been appropriately connected to a national security investigation. That review will also determine whether the practice discussed by the IG existed anywhere other than in the headquarters unit identified in the report.

In response to the obvious internal control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Any agent who needs to obtain ECPA-protected records on an emergency basis must do so pursuant to 18 USC, section 2702. Section 2702 permits a carrier to provide infor-

mation regarding its customers to the Government if the provider believes in good faith that there is a life or death type emergency that requires disclosure of the records. By FBI policy, a request for disclosure pursuant to that provision generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option. The emergency must also be documented to our files so that the use of the letter can be audited. The policy allows for oral requests, but any oral requests have to be approved and documented to the file.

The IG also examined the misuse of NSLs that had been reported and some that had not as part of the IOB process. As this Committee knows, pursuant to executive order, the President has an Intelligence Oversight Board that receives from the intelligence community the reports of intelligence activities that the agency believes may have been unlawful or contrary to executive order or presidential directive.

The IG found that from 2003 to 2005 the FBI had self-reported 26 potential violations involving NSL authorities. The IG also found, however, a number of potential IOBs in the files it examined that had not been reported to OGC for adjudication. Although press accounts of this report have implied that the IG found massive abuses of the NSL authorities, a careful read of the report does not bear out the headlines. The IG examined 293 NSLs, a reasonably small, non-random sample. We do not suggest that the sample was not a fair sample but only point out that it is questionable from a statistical standpoint to attempt to extrapolate from a very small sample to an entire population.

Of the 293 NSLs the IG examined, 22 were judged to have a potential unreported violation associated with them. Of that 7 percent, 10, or almost 50 percent of that group, were third party errors. That is, the NSL recipient provided the FBI with information that we did not seek. Only 12 of the NSLs examined, or 4 percent of the total group, had mistakes that the IG rightfully attributes to the FBI.

Examining the 12 potential errors that were attributable to the FBI reveals a continuum of seriousness relative to the potential impact of individual rights. Four of them, or just over 1 percent of the sample, were unquestionably serious violations. Specifically, two of the violations involved obtaining full credit reports and counterintelligence investigations, which is not statutorily authorized. One involved issuing a National Security Letter when the authorization for the investigation to which it related had lapsed, and one involved issuing an NSL for information that was arguably content and, therefore, not available pursuant to NSL. The remaining eight potential errors involved lack of attention to detail and did not involve the FBI's seeking or obtaining any information to which it was not entitled.

We do not excuse lack of attention to detail, and I have admonished the lawyers in the field who review NSLs that they must be careful so that they can avoid this sort of error, but we do believe that such mistakes pose different challenges and risks than seeking information to which you are not entitled.

In short, approximately 1 percent of the NSLs examined by the IG had significant errors that were attributable to FBI actions and

that had not been but should have been reported as potential IOB violations. A 1-percent error rate is not acceptable, and we have taken steps to reduce it. Those steps are discussed at length in my written testimony, and I will not repeat them here.

But among the steps I do want to mention is that the Director has ordered a special inspection of all field offices' use of National Security Letters, an inspection that began on Friday. We offer to fully brief the Committee on the results of that inspection when it is complete. Several of the actions we are taking involve changes to FBI rules and policy. Rules will, of course, only eliminate errors if they are followed. The IG's report has painfully demonstrated for us that, while we are good at establishing policy and setting rules, we are not as good as we must be at establishing internal controls and auditing functions to make sure that the rules are followed.

The full parameters of an FBI compliance program have not been set, and the inspection that is currently underway will clearly influence the parameters of the program. In short order, however, the FBI will establish a vigorous, multidisciplinary compliance program that assures as well as any compliance program can that our employees faithfully adhere to all of our rules and policies, particularly those that are designed to protect privacy and civil liberties.

The FBI is acutely aware that the only way we can achieve our mission of keeping the country safe is if we are trusted by all segments of the American public. With events like the London terror attack of 2 years ago, we are all worried about the risk of a catastrophic attack from homegrown terrorists. Our single best defense against such an attack is the eyes and ears of all Americans, but particularly in those segments of the population in which the risk of radicalization is at its highest. We need people in those communities to call us when they hear or see something that looks amiss. We know that we reduce the probability of that call immeasurably if we lose the confidence of any part of the American public.

Mr. CONYERS. Counsel, can you wind down at this point?

Ms. CAPRONI. Yes, sir.

We will put into place a compliance program to maximize the probability that we do not lose the confidence of the American public by dint of the sort of errors highlighted in this report.

I appreciate the opportunity to appear before the Committee and look forward to answering your questions.

Thank you.

[The prepared statement of Ms. Caproni follows:]

PREPARED STATEMENT OF VALERIE CAPRONI

Good morning Mr. Chairman, Ranking Member Smith, and Members of the Committee. It is my pleasure to appear before you today to discuss the recent report by Department of Justice's Office of the Inspector General (OIG) regarding the FBI's use of national security letters (NSLs). The OIG's report is a fair report that acknowledges the importance of NSLs to the ability of the FBI to conduct the national security investigations that are essential to keeping the country safe. Importantly, the OIG found no deliberate or intentional misuse of the national security letter authorities, Attorney General Guidelines or FBI policy. Nevertheless, the OIG review identified several areas of inadequate auditing and oversight of these vital investigative tools, as well as processes that were inappropriate. Although not intentionally, we fell short in our obligations to report to Congress on the frequency with which we use this tool and in the internal controls we put into place to make sure that it was used only in accord with the letter of the law. Director Mueller concluded from the OIG's findings that we must redouble our efforts to ensure that

there is no repetition of the mistakes of the past in the use of these authorities and I share his commitment. I would also like to acknowledge the role of Congress and the effectiveness of congressional oversight in surfacing the deficiencies raised in this audit, which was called for in the USA PATRIOT Improvement and Reauthorization Act. The report made ten recommendations in response to the findings, designed to provide both the necessary controls over the issuance of NSLs and the creation and maintenance of accurate records. The FBI fully supports each recommendation and concurs with the Inspector General that, when implemented, these reforms will ensure full compliance with both the letter and the spirit of the authorities entrusted to the Bureau.

NATIONAL SECURITY LETTERS

National Security Letters generally permit us to obtain the same sort of documents from third party businesses that prosecutors and agents obtain in criminal investigations with grand jury subpoenas. Unlike grand jury subpoenas, however, NSL authority comes through several distinct statutes and they have specific rules that accompany them. NSLs have been instrumental in breaking up cells like the "Portland Seven," the "Lackawanna Six," and the "Northern Virginia Jihad." Through the use of NSLs, the FBI has traced sources of terrorist funding, established telephone linkages that resulted in further investigation and arrests, and arrested suspicious associates with deadly weapons and explosives. NSLs allow the FBI to link terrorists together financially, and pinpoint cells and operatives by following the money.

The NSL authority used most frequently by the FBI is that provided by the Electronic Communications Privacy Act (ECPA). Through an ECPA NSL, the FBI can obtain subscriber information for telephones and electronic communications and can obtain toll billing information and electronic communication transaction records. Significantly, the FBI cannot obtain the content of communications through an ECPA NSL. Although the exact numbers of ECPA NSLs remains classified, it is the most common NSL authority used.

Pursuant to the Right to Financial Privacy Act (RFPA), the FBI also has the authority to issue NSLs for financial records from a financial institution. RFPA NSLs are used commonly in connection with investigations of potential terror financing.

Pursuant to the Fair Credit Reporting Act, the FBI has the authority to issue three different, but related, types of NSLs to credit reporting agencies: an NSL pursuant to 15 U.S.C. 1681u(a) for the names of financial institutions with which the subject has or has had an account; an NSL pursuant to 15 U.S.C. 1681u(b) for consumer identifying information (name, address, former addresses, employment and former employment); an NSL pursuant to 15 U.S.C. 1681v for a full credit report. Of all the FBI's NSL authorities, only the last of the FCRA authorities is restricted to use only in international terrorism cases.

Finally, the FBI has the authority to issue NSLs pursuant to the National Security Act in the course of investigations of improper disclosure of classified information by government employees.

For the first 3 types of NSLs (ECPA, RFPA, FCRA) the NSL must include a certification by an authorized FBI employee that the material is being sought for an authorized national security investigation. That certification is slightly different in the case of a FCRA NSL for a full credit report, where the certification required is that the information is relevant to an international terrorism investigation.

The authority to issue an NSL lies at a senior level within the FBI. An NSL can be issued only by an official who ranks not lower than Special Agent in Charge or Deputy Assistant Director. All such officials are career government employees who are members of the Senior Executive Service. Procedurally, an agent or analyst seeking an NSL must prepare a document (an electronic communication or EC) in which the employee lays out the factual predicate for the request. The factual recitation must be sufficiently detailed so that the approving official can determine that the material sought is relevant to an investigation. Additionally, it needs to provide sufficient information concerning the underlying investigation so that reviewing officials can confirm that the investigation is adequately predicated and not based solely on the exercise of First Amendment rights. Finally, the EC includes a "lead" to the Office of the General Counsel (OGC) for purposes of Congressional reporting.

OIG REPORT

As directed by Congress, we endeavored to declassify as much information as possible concerning our use of NSLs in order to allow the maximum amount of public awareness of the extent of our use of the NSL tool consistent with national security concerns. To that end, for the first time the public has a sense of the frequency with

which the FBI makes requests for data with national security letters. In the period covered by the report, the number of NSL requests has ranged from approximately 40,000 to 60,000 per year and we have requested information on less than 20,000 persons per year. For a variety of reasons that will be discussed below, those numbers are not exact. Nevertheless, they, for the first time, allow the public to get some sense of the order of magnitude of these requests; there are a substantial number of requests, but we are not collecting information on hundreds of thousands of Americans.

There are three findings by the OIG that are particularly disturbing, and it is those three findings that I wish to address this morning: (1) inaccurate reporting to Congress of various data points we are obligated to report relative to NSLs; (2) the use of so-called exigent letters that circumvented the procedures required by ECPA; and (3) known violations (both previously self-reported by FBI and not previously reported) of law and policy with regard to usage of NSLs.

CONGRESSIONAL REPORTING

A finding of the report that particularly distresses me is the section that addresses the inaccuracies of the numbers we report to Congress. That responsibility lies with my division, and we did not do an acceptable job. The process for tabulating NSLs simply did not keep up with the volume. Although we came to that realization prior to the OIG report and are working on a technological solution, that realization came later than it should have.

At some point several years before my tenure at the FBI began, our process for tracking NSLs for Congressional reporting purposes shifted from a totally manual process, where NSL data was written on index cards, to a standalone Access database. This database is referred to in the OIG report as the OGC database. While the OGC database was a giant technological step forward from 3 x 5 index cards, it is not an acceptable system given the significant increase in use of NSLs since 9/11. First and foremost, the OGC database is not electronically connected to ACS, the system from which we derive the data. Instead, there is a manual interface between ACS and the OGC database. An OGC employee is responsible for taking every NSL lead that is sent to OGC and manually entering the pertinent information into the OGC database. Nearly a dozen fields must be manually entered, including the file number of the case in which the NSL was issued (typically 15 digits and alphanumeric identifiers).

Approximately a year ago we recognized that our technology was inadequate and began developing an automated system to improve our ability to collect this data. The system, in addition to improving data collection, will automatically prevent many of the errors in NSLs that we will discuss today. We are building an NSL system to function as a workflow tool that will automate much of the work that is associated with preparing NSLs and the associated paperwork. The NSL system is designed to require the user to enter certain data before the workflow can proceed and requires specific reviews and approvals before the request for the NSL can proceed. Through this process, the FBI can automatically ensure that certain legal and administrative requirements are met and that required reporting data is accurately collected. For example, by requiring the user to identify the investigative file from which the NSL is to be issued, the system will be able to verify the status of that file to ensure that it is still open and current (e.g. request date is within six months of the opening or an extension has been filed for the investigation) and ensure that NSLs are not being requested out of control or administrative files. The system will require the user to separately identify the target of the investigative file and the person whose records are being obtained through the requested NSL, if different. This will allow the FBI to accurately count the number of different persons about whom we gather data through NSLs. The system will also require that specific data elements be entered before the process can continue, such as requiring that the target's status as a United States Person or non-United States Person be entered. The system will not permit requests containing logically inconsistent answers to proceed.

The NSL system is being designed so that the FBI employee requesting an NSL will enter data only once. For example, an agent or analyst who wishes to get telephone toll billing records will only have to prompt the system that he is seeking an ECPA NSL for toll records and type the telephone number once. The system will then automatically populate the appropriate fields in the NSL and the authorizing EC. The system will then generate both the NSL and the authorizing EC for signature, thereby ensuring that the two documents match exactly and minimizing the opportunity for transcription errors that give rise to unauthorized collections that must be reported to the Intelligence Oversight Board (IOB). Agents and analysts will still be required to provide the narrative necessary to explain why the NSL is

being sought, the factual basis for making a determination that the information is relevant to an appropriately predicated national security investigation, and the factual basis for a determination whether the NSL should include a non-disclosure provision. In addition, this system will have a comprehensive reporting capability.

We began working with developers on the NSL system in February 2006 and we are optimistic that we will be able to pilot it this summer and roll it out to all field offices by the end of the year. At that point, I will be confident the data we provide to Congress in future reports is as accurate as humanly possible.

In the meantime, we are taking several steps to correct the numbers we have previously reported. First, we are making data corrections in our database. Through a computer program, we have identified all entries that must be erroneous because there is an apparent error in the entry (e.g., there are more NSLs reported than requests; the date shows a year that is impossible (203)). We are manually reviewing those entries and making corrections. We have also started a random sampling of ten percent of the total entries in the OGC database which contains approximately 64,000 entries. Those entries will be manually checked against ACS. We will determine whether there is a significant difference between the entries in our database and the actual information in ACS. To the extent there is a difference, that will be the factor that will be used to correct our prior reporting. While not yielding an exact count, we believe that to be a statistically appropriate way of correcting prior reporting. We have discussed this methodology with the OIG and will offer it the opportunity to review our work. We are striving to have corrected reports to Congress as soon as possible.

As with the other shortcomings identified by the OIG, there was no finding of an intent to deceive Congress concerning our use of NSLs. In fact, as noted, we identified deficiencies in our system for generating data prior to the initiation of the OIG's review and flagged the issue for Congress almost one year ago. While we do not know the extent of the inaccuracies in past reporting, we are confident that the numbers will not change by an order of magnitude.

EXIGENT LETTERS

The next significant finding of the OIG involved the use within one unit at Headquarters of so-called "exigent letters." These letters, which numbered in excess of 700, were provided to telephone companies with requests for toll billing information regarding telephone numbers. All of the letters stated that there were exigent circumstances. Many of the letters stated that federal grand jury subpoenas had been requested for the records even though in fact no such request for grand jury subpoenas had been made, while others promised future national security letters. From an audit and internal control perspective, the FBI did not document the nature of the emergency circumstances that led it to ask for toll records in advance of proper legal process, did not keep copies of all of the exigent letters it provided to the telephone companies, and did not keep records showing that it had subsequently provided either the legal process promised or any other legal process. Further, based on interviews the OIG conducted, some employees indicated that there was not always any emergency relating to the documents that were sought.

OGC has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record we have in an FBI database was obtained because it was relevant to an authorized investigation and that appropriate legal process has now been provided. As of late last week, there were still a small handful of telephone numbers that had not been satisfactorily tied to an authorized investigation. If we are unable to determine the investigation to which those telephone numbers relate, they will be removed from our database and destroyed.

The OIG rightfully objected to the FBI obtaining telephone records by providing a telephone carrier with a letter that states that a federal grand jury subpoena had been requested when that was untrue. It is unclear at this point why that happened. The Director has ordered a special inspection in order to better understand the full scope of internal control lapses.

We also concur with the OIG that it is inappropriate to obtain records on the basis of a purported emergency if, in fact, there is no emergency. We continue to believe, however, that providers had the right to rely on our representation that there was an emergency and that the "exigent letters"—had they been issued only when there was an exigent circumstance and had they correctly identified the legal process that would follow—would have been an appropriate tool to use.

In response to the obvious internal control lapses this situation highlights, changes have already been made to ensure that this situation does not recur. Any agent who needs to obtain ECPA-protected records on an emergency basis must now

do so pursuant to 18 U.S.C. 2702. Section 2702(c)(4) permits a carrier to provide information regarding its customers to the government if the provider in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency. A request for disclosure pursuant to that statute generally must be in writing and must clearly state that the disclosure without legal process is at the provider's option. The letter request must also set out the basic facts of the emergency so that the provider can make some assessment whether it concurs that there is an emergency.

INTELLIGENCE OVERSIGHT BOARD PROCESS

The OIG also examined misuse of NSLs that had been reported (and some that had not been reported) as part of the IOB process. As this committee knows, pursuant to Executive Order 12863 the President has an Intelligence Oversight Board that receives from the agencies in the intelligence community reports of intelligence activities that the agency believes may have been unlawful or contrary to Executive Order or Presidential Directive. This language is interpreted by the FBI and DOJ to mandate the reporting of any violation of a provision of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection if such provision is designed to ensure the protection of individual rights.

The FBI requires its employees to report any violations of law or policy about which they are aware. We encourage employees to err on the side of reporting so that we can be sure that all violations are appropriately reported. In terms of process, all potential violations (called PIOBs—or potential intelligence oversight board violations) are reported to OGC. Lawyers within OGC are responsible for "adjudicating" the violation—that is, determining whether the PIOB is an actual Intelligence Oversight Board violation. If it is, a report is made to the IOB, a copy is provided to DOJ and a copy is provided to the FBI's Inspection Division. If the violation involved intentional misconduct, the Inspection Division will determine whether the matter should be referred to the Office of Professional Responsibility for discipline.

The OIG found that from 2003 through 2005, the FBI had self-reported 26 potential violations involving NSL authorities. Of the 26, OGC adjudicated 19 to be violations and reported them. The OIG agreed with each of those determinations. Of the 7 PIOBs that OGC determined were not violations, the OIG agreed with all but one. As to the one determination about which we disagreed, upon re-review, the FBI concurred with the OIG that it was a violation that should have been reported and it has since been reported to the IOB. These 20 violations included: third party errors (4), NSLs issued when the authority for the investigation had lapsed (3), obtaining ECPA-protected records without any legal process (3) and obtaining a full credit report in a counterintelligence case (1).

The OIG also found, however, a number of potential IOBs in the files it examined that had not been reported to OGC for adjudication. Although press accounts of the reports have implied that the OIG found massive abuses of the NSL authorities by the FBI, a careful read of the report reflects a different set of facts. The OIG examined 293 NSLs—a reasonably small sample. The sample was a judgmental sample and the size was chosen because the audit was extremely labor intensive. We do not suggest that the sample was not a fair sample (although it was not random), but only that it is questionable from a statistical standpoint to attempt to extrapolate from a very small sample to an entire population. Moreover, there was wide variation in the number of purported unreported violations from different field offices. The OIG found 8 potential violations that were unreported in files in both the Philadelphia and Chicago field offices, but only 2 unreported potential violations from files in New York and 4 from San Francisco. We are doing additional follow-up work, but the wide variance between field offices may be a function of the very small sample, or it may indicate that the percentages of potential errors detected are not constant across all field offices.

Setting aside questions about whether the sample is representative, I urge you to look closely at the numbers before arriving at the conclusion that there is a systemic problem concerning the use of NSLs. Of the 293 NSLs the OIG examined, 22 (7%) were judged to have potential unreported IOB violations associated with them. Moreover, of that 7%, 10—or almost 50%—were third party errors—that is, the NSL recipient provided the FBI information we did not seek. Only 12 of the NSLs examined—4%—had mistakes that the OIG rightfully attributes to the FBI.

Examining the 12 potential errors that were rightfully attributed to the FBI reveals a continuum of seriousness relative to the potential impact on individual rights. Four (or just over 1% of the sample) were serious violations. Specifically, two

of the violations involved obtaining full credit reports in counterintelligence investigations (which is not statutorily authorized), one involved issuing an NSL when authorization for the investigation to which it related had lapsed, and one involved issuing an NSL for information that was arguably content, and therefore not available pursuant to an NSL. (In the latter case, the ISP on which the NSL was served declined to produce the requested material so there was, in fact, no collection of information to which we were not entitled.) The balance of the 12 potential violations identified by the OIG do not, in our view, rise to the same level of seriousness as those 4. The remaining 8 involve errors that are best characterized as arising from a lack of attention to detail, and did not result in the FBI seeking or obtaining any information to which it was not entitled. Those 8 potential violations involved errors such as using the wrong certification language in an NSL (although the appropriate certification is not materially different) and having the NSL and the EC seeking the NSL not entirely consistent. We do not excuse such lack of attention to detail, but we do not believe that such mistakes result in or cause a risk to civil liberties.

In short, approximately 1% of the NSLs examined by the OIG had significant errors that were attributable to FBI actions and that had not been, but should have been, reported as PIOBs.

While a 1% error rate is not huge, it is unacceptable, and we have taken steps to reduce that error rate. First, we are very concerned that of all the potential IOBs involving mistakes in NSLs attributable to the FBI (whether previously reported or not), 3 involved the same mistake: namely, issuing an NSL for a full credit report in a counterintelligence investigation. In order to ensure that this particular error is fully rectified, the FBI ordered all field offices to examine all counterintelligence files in which Fair Credit Report NSLs have been issued since January 1, 2002 in order to ascertain whether the file contains a full credit report. If it does, the credit report must be removed from the file, sequestered with the field office's attorney, and a PIOB must be reported to OGC. The results from that search are due to headquarters by April 16, 2007.

Several other steps we have taken will, we believe reduce the likelihood that the FBI will commit the other mistakes in the future. First, as indicated previously, the FBI is developing an automated system to prepare NSLs and their authorizing ECs. That system will reduce to zero mistakes such as having the wrong certification language or inconsistency between the NSL and the EC. It will also ensure that the investigative file out of which the NSL is being issued is open. Finally, it will ensure that an NSL for a full credit report cannot be issued out of a counterintelligence file.

Other changes to FBI policy have been made that we believe will facilitate better handling of IOBs and also reduce errors that lead to IOBs. First, last fall we provided comprehensive advice to the field regarding its responsibility towards information obtained as a result of third party errors. That guidance requires all such information to be sequestered and reported to OGC as a PIOB. If the "over collected" information is irrelevant to the investigation (e.g., the telephone company transposed a number and provided us records on the wrong telephone account), then it will be destroyed or returned. No such information should be entered into FBI databases. If the information is relevant to the investigation but simply not within the four corners of the NSL, then the information must be sequestered until a new NSL has been issued for the extra data. After the new NSL has been issued, the information can be entered into FBI databases.

Secondly, we have collected all the rules and policies on NSLs into one document which will be disseminated to the field. Those rules now mandate that, until the deployment of the automated NSL system, all NSLs and ECs be prepared from the exemplars that are provided on OGC's website. That should eliminate many of the mistakes identified by the OIG.

All of these rules will, of course, only reduce or eliminate errors if they are followed. The OIG's report has highlighted for us that there must be some sort of auditing function—above and beyond the IOB process—to systematically ensure that these rules, as well as others that govern our activities in national security investigations are followed. The FBI has historically been very good at establishing policy and setting rules, but we have not been as proactive as we should have been in establishing internal controls and auditing functions.

The full parameters of the compliance program have not been set, although these aspects have been: the Inspection Division with participation of DOJ's National Security Division and Privacy and Civil Liberties Office is in the process of a special inspection of NSL usage in all 56 field offices and headquarters. That inspection should uncover any other significant problems with our use of this tool but should also tell us whether there are variances between offices in terms of the numbers and types of errors. The results of the inspection will then inform the program that

the Attorney General announced of having teams of DOJ lawyers, FBI lawyers and the Inspection Division periodically audit field offices' use of NSLs. That process will begin in April and should result in at least 15 offices being audited this year. We are also considering other proactive compliance programs in order to develop a program that ensures, to the maximum extent possible, that the rules and policies designed to protect privacy and civil liberties are faithfully adhered to by all of our employees, that we promptly identify and correct any violations of law or policy, and that any information collected erroneously is removed from FBI databases and destroyed. In addition, a working group co-chaired by the Office of the Director of National Intelligence and the CPCLO has been convened to examine how NSL-derived information is used and retained by the FBI. The FBI and DOJ's National Security Division will have a representative on this working group. We welcome the Committee's input as we move forward on these initiatives.

The FBI is acutely aware that the only way that we can achieve our mission of keeping the country safe is if we are trusted by all segments of the American public. With events like the London terror attacks of 2 years ago and the Canadian plot to use fertilizer bombs to destroy buildings in Canada in 2006, we have all become worried about the risk of a catastrophic attack from home grown terrorists. Our single best defense against such an attack is the eyes and ears of all Americans—but particularly of those segments of the population in which the risk of radicalization is at its highest. We need people in those communities to call us when they hear or see something that looks amiss. We know that we reduce the probability of that call immeasurably if we lose the confidence of those segments of the population. That is one of the reasons that we are looking for ways to assure all Americans that we are respectful of individual rights, including privacy rights, and that we use the tools that have been provided to us consistent with the rules set out by Congress.

I appreciate the opportunity to appear before the Committee and look forward to answering your questions.

Mr. CONYERS. Well, General Counsel Caproni, I want to thank you for your candor and forthcomingness in coming before us today, and we will include the rest of your testimony, of course.

Now let me begin the questioning, and I thank both the witnesses.

Inspector General Fine, I am curious as to how you have come to the conclusion that these errors that have been reported and that bring us to this chamber were sloppy—the results of sloppy bookkeeping, recordkeeping or compliance with the law, but none of it was intentional.

How could that be if they have known about these excesses since the year 2004, and their Communications Analysis Unit warned them about it in early 2005, and we have something like at least over 700 Exigent Letters and somewhere in the neighborhood of 40,000 to 50,000 NSL letters for 3 years?

Mr. FINE. Let me separate some of those issues.

I do not believe that they intended to go out and to obtain information that they knew they could not obtain and said, "We are going to do it anyway."

I think what they did was complete carelessness; they did not follow the rules, did not follow appropriate procedures, and obtained information that they could have obtained properly but by taking shortcuts. Now, we did not do a review to ask everybody what was in their minds and what exactly they did, but we saw instances where people just simply did not follow the rules and did not take appropriate action.

Mr. CONYERS. But they were being warned. This did not just come up recently. This goes back to 2004.

Mr. FINE. In 2004, it is correct that attorneys in the Office of General Counsel had concerns about the Exigent Letters and were

not saying "stop it," but were saying "we need to take different measures to issue these letters."

Mr. CONYERS. Do you think that the law was so complicated that people in good faith just could not figure out what it was we were requiring?

Mr. FINE. I think what they did was inappropriately take a model from another context and apply it to this context, which was wrong—it clearly was—and that they did not think carefully, and they did not take appropriate actions. Now, I know that the FBI is conducting a special inspection to look at exactly what everybody knew and when they knew it and why they took the actions that they did. We did not do that kind of review. We did not ask everybody up and down the line, and it is possible that people had motivations that were not appropriate.

Mr. CONYERS. But there is no way we can tell. There is no way I can tell, but there is no way you can tell either.

Mr. FINE. It is true that we did not do a performance review of every individual, so I think that is an appropriate point, Mr. Chairman—I really do—and I do think it is incumbent upon the FBI to go back and look and see exactly what people were doing, at what stages, and why they did, what they did and take appropriate action to hold people accountable.

Mr. CONYERS. Now, do you make a distinction between the National Security Letters and the Exigent Letters in terms of the severity of the offense that brings us here today?

Mr. FINE. I think I do. I think the Exigent Letters were the most troubling aspect of this.

Mr. CONYERS. And why is that?

Mr. FINE. Because there is a process in the law to allow voluntary disclosures from these telephone companies if there is a true emergency, and we believe the FBI should have followed that voluntary process. Instead, they went with these Exigent Letters, which they used in a different context, and applied it to this context which, in our view, was inappropriate.

With regard to the National Security Letters, there were many of them, and many of them did comply with the requirements of the law. We saw, and we tried to do a review to see how many did not. We found a significant number did not, but with regard to the Exigent Letters as a whole, that whole practice was very troubling to us in and of itself.

Mr. CONYERS. Now, are you satisfied with the steps that have been described here today by the General Counsel in terms of how we clean this mess up?

Mr. FINE. Well, we have been briefed by the Department and the FBI about the steps they are taking. I think they are taking this seriously, but I am not in a position right now to say, "I am completely satisfied. I trust all this." We need to see what happens with these steps, see whether there are concerted efforts over time, to see whether they really are adequately implemented. So I cannot say right now that they have done all they can, but I think they are taking important steps and taking this very seriously.

Mr. CONYERS. I thank you so much.

I recognize Lamar Smith.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Chairman, I am hoping my first question will not count against my time.

Mr. Fine, I noticed, in reading your bio that when you were a senior in college and co-captain of the basketball team you were recruited by the San Antonio Spurs. They happen to be my hometown team. My question is this: Don't you regret not playing for the Spurs rather than becoming a Rhodes scholar and graduating from Harvard Law School?

Mr. CONYERS. The gentleman's time has expired.

Mr. FINE. Congressman, I was drafted in the 10th round by the San Antonio Spurs, and if I were maybe a little taller than 5′9″, I might have had a chance to play. So I do not really regret that my future was in the law rather than in professional basketball. But I tell people who do not believe I actually played basketball when they see me at 5′9″ that before I started this job as the IG I was 6′9″.

Mr. SMITH. A very good answer.

Mr. Fine and Ms. Caproni, let me address a more serious question to both of you, and it is this. We have unearthed these problems that are recognized and that are being dealt with, and some of the reasons for those problems have already been seen, and the practice has been discontinued, but my question is this:

Do you all feel that the problem is with how the law was enforced rather than with the law itself? In other words, if the law were carried out as intended, doesn't that solve our problem? Mr. Fine first.

Mr. FINE. Congressman, I am really not in a position to say what the law should be or if there should be modifications to the law.

What my job is is to look at the law and to look at the application of the law and to see the problems that occurred. I do believe that if the FBI had assiduously and carefully applied the law, we would not have seen as many problems as we have, and it really was unacceptable and inexcusable what happened here.

Mr. SMITH. Ms. Caproni.

Ms. CAPRONI. From our perspective, the problem is not with the law, although I would note that unlike other areas that our agents, where they get these sorts of records, there are very specific rules, and they have to win through those rules. That, in my sense, is our responsibility as the lawyers to make sure that the agents understand what they can do and what they cannot do.

Again, there is no doubt that the problem with the National Security Letters was a colossal failure on our part to have adequate internal controls and compliance programs in place. The laws, themselves, provide us with a needed tool, and it is a tool that we should use responsibly.

Mr. SMITH. Okay. Thank you.

Mr. Fine and Ms. Caproni, why are National Security Letters important in our investigation of terrorism?

Ms. CAPRONI. They are critical. National Security Letters provide us the basic building blocks that we need to build an investigation. For those of you who had prior criminal AUSA experience—and I know a number of you did—you are used to issuing grand jury subpoenas to obtain telephone records and banking records. Frequently in terrorism investigations, we do not have an open crimi-

nal investigation. In fact, that was one of the things that the 9/11 Commission really encouraged us to do and that this Committee encouraged us to do and the intelligence Committees, to move more—when we are thinking about a terrorism case, to move from simply a criminal mindset to thinking in an intelligence mindset. So a National Security Letter is the tool that we use in order to get the basic building blocks of those investigations, again, like phone records for almost every terrorism case, financial records when we are building terrorism financing cases. So, without National Security Letters, our national security investigations would really be stopped before they even got started.

Mr. SMITH. Okay. Thank you.

Mr. Fine.

Mr. FINE. I do think that they are important investigative tools. They can connect terrorist individuals with terrorist groups. They can find out where terrorist financing can occur. They are indispensable in counterintelligence investigations. And the FBI did tell us, from folks in the field to headquarters, how important they were to the investigations and showed us examples of that. I have said that I think they are important. There also needs to be important checks on these tools because they are intrusive, and there is information that is obtained and retained for significant periods of time, and so while they are important investigative tools, there also needs to be appropriate checks on them as well.

Mr. SMITH. Mr. Fine, in your conclusions—it is the second one—you say, "In most but not all of the cases we examined in this review, the FBI was seeking information that it could have obtained properly through National Security Letters."

What percentage would you guess is that? In other words, what percentage of the problems could have been resolved if they had obtained National Security Letters?

Mr. FINE. We found instances, a few instances, where they obtained information inappropriately and could not have used a——

Mr. SMITH. How many of the 739 would you guess that is?

Mr. FINE. Well, the 739 is hard to tell because they could not tie them to appropriate investigations all the time, and there were many times where they could not tell us it was an emergency, so I do not know how many in the 739. That is the most troubling aspect of it.

With regard to the others, the National Security Letters in the files we reviewed, I would say we found about seven where there were illegal uses of them, where the FBI was attempting to obtain information through confusion, through error, of information that they were not entitled to obtain through a National Security Letter, either an educational record or obtaining information on a full credit report in a counterintelligence case, which they are not allowed to obtain, or not using it in NSL——

Mr. SMITH. You said seven times?

Mr. FINE. Seven of the reviews that we found and we found in our—seven of the individual ones, and as you will recall, we did not do a review of every NSL that was issued. We did a small sample of them.

Mr. SMITH. Okay. Thank you, Mr. Fine.

Thank you, Mr. Chairman.

Mr. CONYERS. Thank you very much.

The gentleman from New York, Jerry Nadler.

Mr. NADLER. Thank you.

Well, Mr. Fine, I suppose. You state in your report that there were no intentional violations of NSL policy procedure, that these were basically carelessness but that there were no intentional violations, no crimes.

Mr. FINE. Correct.

Mr. NADLER. Okay, but we also read in the report that agents intentionally went around the statute to provide phony information requests to telephone companies based on false statements.

For example, the FBI's Communications Analysis Unit went around the NSL statute because it felt that the statute was insufficient and contracted with the telephone companies to access information directly. These contracts were approved by the Office of General Counsel and were exploited by issuing Exigent, or emergency, Letters. Well, let me ask the General Counsel.

What is the statutory basis for an Exigent Letter? As far as I can tell, there is no basis for it.

Ms. CAPRONI. Well, under 2702, we have the authority to get records from a phone company in an emergency circumstance without a National Security Letter. The Exigent Letters were undoubtedly inappropriate shortcuts to the process, though.

Mr. NADLER. Well, under 2702, if you were going to get information in an emergency, what do you have to do?

Ms. CAPRONI. You simply have to tell the carrier that there is an emergency. We recommend that you explain to the carrier what the emergency is, and it is then up to the carrier to decide whether or not to provide us records. So it is not a compulsive system.

Mr. NADLER. Not compulsive, but of course, the carrier has no particular interest in protecting—if you are looking at my records or if you want my records, for example, the phone company has no particular interest in protecting my privacy rights, and I will never find out about it, so I cannot go to court to protect them, correct?

Ms. CAPRONI. I do not represent the carriers, but I would disagree with the theory that they have no particular interest in protecting your records. In fact——

Mr. NADLER. What is their interest?

Ms. CAPRONI. In fact, the carriers were diligent in making sure that any record they gave to us they subsequently obtained a National Security Letter for.

Mr. NADLER. Well, wait a minute. Mr. Fine's report says, in many, many instances, hundreds of instances, that that never happened.

Ms. CAPRONI. As of right now, there are still some numbers that have not received National Security Letters to back up the requests.

Mr. NADLER. But back up years later after the report, but that is backfilling, in other words, and that is certainly not evidence that the phone companies were diligent in seeking these things. That is saying that, after this report was done, someone said, "Wow, we have got a problem on our hands. We had better go get these letters 4 years later or 3 years later." That is not evidence of what we are talking about.

Ms. CAPRONI. Respectfully, even though I am not defending the practice, it is not the case that it was only after Mr. Fine's report came out that they were attempting to make sure that the paperwork documentation was appropriate for every record they obtained.

Mr. NADLER. You think the paperwork documentation should be done as appropriate.

Ms. CAPRONI. If it is not, the records will come out of our database and be destroyed.

Mr. NADLER. In this morning's Washington Post, it says: Under past procedures agents sent exigent circumstances letters to phone companies seeking toll records by asserting there was an emergency. Then they were expected to issue a grand jury subpoena or national security letter which legally authorizes collection after the fact. Agents often did not follow up with that paperwork, the Inspector General's investigation found.

The new instructions which, according to the Washington Post, were issued to the FBI tell agents there is no need to follow up with National Security Letters and subpoenas. The agents are also told that the new letter template is the preferred method in emergencies but that they may make requests orally with no paperwork sent to phone companies.

In other words, it appears from this morning's Washington Post that instructions are now being given to the FBI not to bother with any backup documentation after an oral request to the phone company for records invading people's privacy.

Ms. CAPRONI. Quite the contrary. The instructions are that if they get information based on an oral request—and just to give an example of when that might be appropriate, if a child has been kidnapped and the ransom call comes in——

Mr. NADLER. Obviously, in those—I am not questioning the need in an emergency like that for getting records right away.

Ms. CAPRONI [continuing]. And to get them on an oral request.

Mr. NADLER. I don't doubt it. What I am questioning is that, according to today's Washington Post, the opposite of what the two of you are saying is the case and that now they seem to be saying we will take care of this lack of follow-up of documentation by simply declaring it unnecessary.

Ms. CAPRONI. No, Congressman, that is not the policy. The policy now is that if a request is going to be made on an emergency basis for records, that has to be documented. It has to be documented in the first instance in the request. But if there is not time to do that so that you need an oral request, then that has to be documented to the file together with the approval for it. So it is, again, an internal control to avoid the problem that was existing, which was emergency had become a flexible——

Mr. NADLER. Okay. One final question. That is to Mr. Fine. Just a quick clarification on accessibility of PIN numbers and Social Security numbers of individuals through this process.

On page 73 of your report, there is a discussion of a potential Intelligence Review Board violation because an agent accessed a bank balance by getting a person's bank account and PIN number from the result of a FISA order. The agent was faulted for not using an

NSL but was not faulted for the fact that the PIN number was readily available.

The reason I flagged this is because this reference makes clear that through an NSO 215 order the Government can secretly obtain the PIN number for someone's debit or credit account——

Mr. CONYERS. The gentleman's time has expired. Finish.

Mr. NADLER. What limits are there on this and what protections on this power to get PIN numbers and credit account numbers?

Mr. FINE. The FBI can get bank records and records like that. There has to be predication for it and they have to show the need for that. That is one of the tools that the FBI has used and can use, as we pointed out. That is one of the reasons there needs to be controls on this.

Mr. CONYERS. The gentleman's time has expired.

The Chair turns to the former Chairman, Jim Sensenbrenner from Wisconsin, whose letter to the Department of Justice first triggered the inquiries that have flown from this. I congratulate him and recognize him at this time.

Mr. SENSENBRENNER. Thank you very much, Mr. Chairman.

Just by way of background, we did some oversight when I was the Chair of the Committee and received a letter in late 2005 that indicated that there were problems with National Security Letters. The audit that the Inspector General conducted was as a result of a provision that I put in the PATRIOT Act reauthorization that required this audit to be made as well as a subsequent audit that Mr. Fine is doing that I am sure we are going to talk about extensively later when the report is issued.

I would also like to point out that National Security Letters were not authorized by the initial PATRIOT Act in 2001 but have been around since 1986 in legislation that was authored by Senator Patrick Leahy of Vermont, who is the Chairman of the Judiciary Committee on the other side of the Capitol.

The PATRIOT Act reauthorization put in a number of civil liberty protections relative to National Security Letters because we knew that there were problems afoot and decided that, even though NSLs were not a part of the PATRIOT Act, that they needed to have civil liberties protections.

I am proud of that work that this Committee did and eventually found its way into the PATRIOT Act Reauthorization Act, which was signed by the President in March of last year.

One of the things, Ms. Caproni, that I am really concerned about is that the Justice Department and the FBI in particular have come to the Congress repeatedly over the last dozen years asking for administrative subpoena authority, meaning that subpoenas could be issued without judicial supervision. This Congress has repeatedly rejected each and every one of those requests.

Now a National Security Letter is kind of like an administrative subpoena, although it is limited to the type of information that can be obtained. I would like to know from both of the witnesses whether the FBI simply turned around and used NSLs to get huge amounts of information after Congress said "no" again to administrative subpoena authority.

Ms. CAPRONI. No, we didn't. National Security Letters are always focused on a particular case. There is no bulk collection via Na-

tional Security Letters. And while our congressional reporting numbers are off, as Mr. Fine correctly found, they are not off by an order of magnitude. That is, we reported that we collected data on less than 20,000 people a year. While that number may go up, it is not going to go up to above 200,000.

Mr. SENSENBRENNER. How can you account for the fact that the number of NSLs that were issued before 9/11 was about 8,000 plus per year and then it went up to 150,000? Do we have that many potential terrorists running around the country? If so, I am really worried.

Ms. CAPRONI. I think it is a function of two things. First off, I think it is a function of the fact that post-9/11 a number of agents were moved into the counterterrorism area and the Director directed that no lead in a counterterrorism case would go unpursued. So there is a directive to agents that they must cover all counterterrorism leads. That is point one.

I think point two was, because we were focusing much more on an intelligence-driven reaction to counterterrorism threats, the toolbox that we were using was focusing mostly on National Security Letters, as opposed to the prior reaction, which would have used grand jury subpoenas.

Mr. SENSENBRENNER. Mr. Fine.

Mr. FINE. I agree with Ms. Caproni. Prior to the September 11th attacks, it was rarely used. There were delays in getting them, and they were not following the leads that they would have followed after the 9/11 attacks.

After the 9/11 attacks, they are attempting to connect the dots, attempting to track down leads. When there are indications from a terrorist overseas that there might be connections to the United States, they try and follow that.

Mr. SENSENBRENNER. My time is running out. I just make the observation that one of the things that gets people in this town in big trouble is overreaching. I think that, given your report, Mr. Fine, the FBI has had a gross overreach. What this does is it erodes support for the function that the FBI does to protect all of us from future terrorist attacks.

I hope that this would be a lesson to the FBI that they can't get away with this and expect to maintain public support for the tools that they need to combat terrorism. Given the way the FBI has acted, I have my doubts. But let this be a warning.

And my time is up.

Mr. CONYERS. The Chair recognizes the gentleman from Virginia, Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Fine, you suggested that there is some confusion in how to work these things, as I understand it, representations that there was an emergency, when in fact there was no emergency, and representations that grand jury subpoenas had been issued, when in fact they had not been issued. Is that right?

Mr. FINE. That is correct.

Mr. SCOTT. Has anyone been sanctioned?

Mr. FINE. No. The FBI, as a result of this report, is going and looking at a special inspection to look at exactly what happened

with this, how the problems occurred, and to determine accountability. I think that is appropriate.

Mr. SCOTT. To your knowledge, no one has been sanctioned so far.

Mr. FINE. Not yet, no.

Mr. SCOTT. Okay. Ms. Caproni, you indicated that we need to change our mindset from criminal investigation to intelligence gathering.

Ms. CAPRONI. I am saying that, post-9/11, that has been what the FBI has been charged with doing—really not thinking of our terrorism investigations as wholly criminal.

Mr. SCOTT. Now when we use these letters, are we obtaining information regarding United States citizens?

Ms. CAPRONI. Sometimes.

Mr. SCOTT. That is a yes? Not always, but sometimes?

Ms. CAPRONI. Correct. About half and half.

Mr. SCOTT. You are using this mindset against United States citizens. When you get all this information like Social Security numbers and phone records, how long is this information retained?

Ms. CAPRONI. The issue of retaining national security—data that is obtained via National Security Letters is subject to a working group that the DNI is chairing together with the Department of Justice and that we will participate on in terms of how long we should keep it. As of right now, it is subject to the normal archive rules, so we keep it for whatever the law under our archives requires, which is typically 20 years.

Mr. SCOTT. Twenty years. Now how many criminal convictions have you gotten from NSL letters? How much information from NSL letters has resulted in criminal convictions for terrorism-related offenses?

Ms. CAPRONI. That was one of the questions that the IG was charged with answering, and I think deriving is very difficult. Because, while National Security Letters are typically used at the beginning of an investigation, we don't tag the data; and so tracing it through to know whether national security data started——

Mr. SCOTT. Mr. Fine.

Mr. FINE. We try, too, but you cannot tell how many convictions as a result of that. It is not specifically segregated or tagged. When we tried to follow through the system, it was very hard to do that. So I can't give you a number.

Mr. SCOTT. If somebody said one, would that surprise you? Could you contest that number?

Ms. CAPRONI. I would.

Mr. FINE. I would think it would be higher, but I can't tell you one way or the other.

Mr. SCOTT. What information is obtained through NSL letters that could not have been gotten through going through the normal FISA process, even in emergencies when there is an after-the-fact process with the FISA courts?

Ms. CAPRONI. Anything that we can obtain through a National Security Letter could be obtained from a FISA 215 order.

I would tell this Committee that I think if you change the law in that way, you would be doing grave disservice. It would essentially sink the system. We issue, as you can tell from the report,

thousands of National Security Letters to get information. We do not have an infrastructure in place to take every one of those to court any more than an AUSA in any district has the infrastructure in place to go to court to get every grand jury subpoena. It is simply—we don't have the infrastructure to do that.

Mr. SCOTT. So you are not getting information you couldn't get through FISA, but just administratively you would have a judge looking at what you are doing and not having a process that lacks oversight.

Ms. CAPRONI. Congressman, under FISA—under the FISA statute, section 215 of the PATRIOT Act gave us the authority to get an order for any type of record.

Mr. SCOTT. That is what we are talking about.

Mr. Fine, did I understand that in these cases there is an actual ongoing investigation prior to issuing these letters or there is not an identifiable investigation ongoing when they issued the letters?

Mr. FINE. It has to be tied to some investigative file. They have to open an investigative file or a threat assessment or preliminary inquiry or full inquiry. It has to be tied to one of those, and can't be issued out of a control file.

Mr. SCOTT. That is what they are supposed to be doing. Are they doing that?

Mr. FINE. We found there were instances of they were issued out of a controlled file.

Mr. SCOTT. If there is no ongoing investigation, what is the standard for deciding when to issue one and when not to issue one?

Ms. CAPRONI. The standard is that it has to be relevant to an authorized investigation. What Mr. Fine was talking about with the control files is, while it is a difficult situation to understand, those NSLs were in fact—they related to an authorized investigation. There was a bureaucratic problem, which nobody likes to hear. There is a bureaucratic problem, but there was a huge bureaucratic problem that we believe we have worked out. None of the NSLs that were issued out of control files did not relate to an authorized investigation. They all were tied to investigations that were appropriately open.

Mr. CONYERS. The distinguished gentleman from North Carolina, Howard Coble.

Mr. COBLE. I thank the Chairman.

Good to have you all with us.

Mr. Fine, your report recommends a number of changes on the FBI's use and tracking of National Security Letters. The Attorney General issued a press release on March 9th responding to those recommendations; and I presume each of you is familiar with that report, are you not, the March 9th report?

Let me put this question to each of you: Will those recommendations submitted by the AG restore the FBI's accountability for its use of NSLs?

Mr. Fine, start with you.

Mr. FINE. I believe that the response to the recommendations and what the FBI and the Department is doing is appropriate. Is it sufficient? Is it all that needs to be done? I am not sure. We will have to see what the results of those steps are.

We try to provide recommendations to ensure that these very important but sensitive tools are used in full accord with National Security Letter authorities, AG guidelines, and internal control policies. They hadn't been in the past.

Mr. COBLE. Ms. Caproni.

Ms. CAPRONI. I think we are going to have to work to get the trust of this Committee back, and we know that is what we have to do, and we will do it.

Mr. COBLE. Can the FBI implement the Attorney General's directions within the 4 months when the AG has requested Mr. Fine to report on your progress?

Ms. CAPRONI. I hope so. There are some that are going to require some interagency work, but certainly if not all will be implemented in 4 months, we will have made substantial progress.

Mr. COBLE. You may have addressed this earlier, Ms. Caproni, but let me put it to you in case you did not. Does the FBI have any discrepancy or challenge with the report that Mr. Fine has issued?

Ms. CAPRONI. No, we accept the report. To the extent we had factual quarrels, we worked those out.

Mr. COBLE. You may not be able to respond to this. What do you think, Ms. Caproni, are the greatest obstacles that your office faces in implementing the AG's directions?

Ms. CAPRONI. I think that any obstacles there are the Director is going to make sure are removed. I think it is time—it is energy and effort; and we are going to do it.

Mr. COBLE. I thank you both for being here.

Mr. Chairman, if I may, I would like to submit for the record the March 9th press release submitted by the Attorney General.

Mr. CONYERS. Without objection, so ordered.

[The information referred to is available in the Appendix.]

Mr. COBLE. I thank the Chairman. I yield back my time.

Mr. CONYERS. I ask the lady—don't sit down now. I ask you to please excuse yourself from this hearing. No visitors can interrupt a hearing in the Congress. Just a moment. Would the officers escort this lady out, please.

The Chair recognizes the other distinguished Member from North Carolina, Mr. Mel Watt.

Mr. WATT. Thank you, Mr. Chairman. I thank the Chairman for convening the hearing.

Mr. Fine, I am looking on page 7 of your testimony in which you indicate that you reviewed 293 National Security Letters in 77 files and found 22 possible violations that had not been identified or reported by the FBI, and I am trying to extrapolate that, although Ms. Caproni seemed to take some issue with whether that was a reliable sample.

I am trying to assume for the moment that it is, without trying to figure out how many there would be of the total National Security Letters that were possible violations.

My formula is I am starting with 143,000 National Security Letter requests on page 5. Would that be an appropriate place to start? Have you done the extrapolation for me?

Mr. FINE. I haven't done it, but there are 143,000 requests, and, as you know, a request—there can be multiple requests in a letter,

so there are approximately 45,000 letters during the time period, with 143,000 requests. I think the starting point would be about 44,000 letters during the time period.

Mr. WATT. And if you extrapolated the possible violation out, what would that come to, according to your math?

Mr. FINE. If you are talking about 7 percent, approximately 7 percent of the 293 had a violation, so 7 percent of 44,000 would approximately be about 3,000.

Mr. WATT. So you are telling me——

Mr. FINE. That is quick math. I hope it is correct. I think it is.

Mr. WATT [continuing]. That it is possible my FBI and my people who are supposed to be protecting my interest violated the law how many times?

Mr. FINE. Well, I think there are possible violations of either the law, the Attorney General guidelines or the FBI's policies several thousand times, if you statistically extrapolate. It was a small sample. We didn't think it was skewed or biased. But if it held up through the entire population of files, several thousand, some more serious than others. But that is a lot.

Mr. WATT. Ms. Caproni, why ought not our public be concerned about that kind of disregard of the law and internal process?

Ms. CAPRONI. Well, I think the public should be concerned. We are concerned, and we are going to fix it.

I would say, as Mr. Fine said, the sort of errors range sort of on a long continuum of seriousness. The most serious errors that Mr. Fine identified were obtaining full credit reports in counterintelligence cases. We had a——

Mr. WATT. That is 7 of the 22 files where you say they were real serious violations. Extrapolate that out for me, Mr. Fine.

Mr. FINE. Well, I think in Ms. Caproni's testimony she talked about the level of seriousness and which were FBI errors and which were company errors and came up with the figure that a little bit over 1 percent of them were serious violations involving FBI errors. If you extrapolate that to the entire population, that would be about 600 cases of serious FBI misconduct.

Mr. WATT. Ms. Caproni, is there some reason that this Committee and the American public shouldn't be concerned about law enforcement violating the law 600 times?

Ms. CAPRONI. We are quite concerned about this, Congressman; and we are making every effort to figure out where those errors are, to sequester the material, to pull it out of our files and to destroy it. We will——

Mr. WATT. How many files have you all destroyed based on this investigation up to this point?

Ms. CAPRONI. When we identify data that——

Mr. WATT. Isn't that a number rather than an explanation?

Ms. CAPRONI. Congressman, I don't know the number.

Mr. WATT. Has the FBI destroyed any files up to this point based on this investigation?

Ms. CAPRONI. We destroy data all the time when we discover it was improperly collected. So both outside of Mr. Fine's investigation and——

Mr. WATT. Have you destroyed any files based on this investigation?

Ms. CAPRONI. Again——

Mr. WATT. Have you destroyed any file?

Ms. CAPRONI. Not a file.

Mr. WATT. Have you destroyed any information based on this investigation?

Ms. CAPRONI. Yes.

Mr. WATT. What have you destroyed?

Ms. CAPRONI. The full credit reports that were obtained improperly, and I think there was also some telephone data.

Mr. WATT. How many is that?

Ms. CAPRONI. It is not much.

Mr. WATT. In these 600 cases that you have identified as possible real serious areas, several hundred, do you intend to prosecute anybody for violating the law?

Ms. CAPRONI. We will have to look at what the facts are. I am not going to pre-judge.

Mr. WATT. How long is it going to take you to look at that?

Mr. CONYERS. The gentleman's time has expired.

Ms. CAPRONI. The inspectors are in the field now, and I think they will have completed their inspection, which is a sampling process, but they will have completed it within a week or so.

Mr. WATT. You have got a more reliable sampling process than Mr. Fine.

Ms. CAPRONI. It is bigger, and it is across all field offices.

Mr. CONYERS. The gentleman from California, once an attorney general for his State, Dan Lungren.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Ms. Caproni, I was one of the ones who have defended the FBI and the Justice Department in the use of these as we went through legislation the last 2 years, and to say that I am disappointed doesn't give justice to what I feel about this.

Mr. Fine has said that this is the result of mistakes, carelessness, confusion, sloppiness, lack of training, lack of adequate guidance and lack of adequate oversight. That sounds like a report about a first or second grade class. We are talking about agents of the FBI, who are lawyers in many cases, who have college degrees, who have other kinds of education. We are talking about people who have gone through the FBI Academy. We are talking about people who presumably have been trained to go into this.

We are how many years past 9/11?

In response to the question I believe it was of Mr.—I am not sure who asked you this, but whether you could get this done in 4 months, you said you hoped so. I hope you will deliver a message that we expect it will be done. Because I don't think if you can't get it done in 4 months you are going to have to worry about improving your procedures for NSLs because you probably won't have NSL authority.

I just want to convey to you how upset many of us are who have defended this program and have believed it is necessary to the protection of our country and you in the FBI have an obligation to try to find out who the potential terrorists are but also to make good on the promise we have made to the people of America that the terrorists are not going to succeed by indirection what they can't do by direction. That is, to destroy the constitution.

I just—I will tell you this. I talked with Mr. Mueller yesterday. Because I have known him for 30 years. He's Mr. Fix-it. He goes in and fixes messes. He has done it all over this Government. I have seen his work in San Francisco. I have seen his work here at the Department of Justice. If I didn't know him, if I didn't know his record, if I didn't know he is the man we have put in many places to fix things, I would have no confidence in the FBI right now.

So I hope you will deliver a message to all your people that it is not good enough to tell us you hope it is going to be done in 4 months. I hope you are going to deliver a message that it better be done in 4 months or you are not going to have NSLs to worry about. I have to say that as someone who supports them and will fight on the floor to have that authority given to you if there is proper oversight. But I probably won't get a majority of votes on the House floor if you don't fix it. So can you tell me you are going to do better than you hope to fix it in 4 months?

Ms. CAPRONI. Congressman, you are absolutely right. Yes, it will be done.

Mr. LUNGREN. I appreciate that.

Now, Mr. Fine, you are the Inspector General for the FBI. I want to congratulate you on what you have done. We say we take some satisfaction in your carrying out the authority we gave you, but sometimes that doesn't happen, and we appreciate the job you have done here.

Maybe you won't want to answer this question. Maybe you can help me. How do you explain carelessness, confusion, sloppiness, lack of training, lack of adequate oversight with the FBI? I just turned on television last night and watched one or two or three of these shows that always shows the FBI as being far better than local government. A little burr under my saddle, because I am a former AG of California. I appreciate the FBI, but how do you explain this? I am not sure what would be worse, frankly.

At first, I was relieved that you said this and that it wasn't intentional action by the FBI. At least, we haven't found that. I would at first have been worried about that.

Now, as I think about this, should I be more worried about the fact that the FBI now, in something as important as NSLs, has marks of carelessness, confusion, sloppiness, lack of training, lack of adequate guidelines and lack of adequate oversight? Is this exceptional in your experience in your oversight of the FBI?

Mr. FINE. I think the FBI worked hard to get these authorities but didn't take it seriously enough putting in controls over these authorities. I think there is often a problem sort of between the receipt of the authority and the execution of that authority. That is clearly what happened here. We were very troubled by it.

We have seen problems in the FBI in terms of information technology and trying to upgrade their information technology. We have seen problems, but they are—these are difficult tasks, and they are trying to do this as they are changing their mission, and, quite honestly, there really is no excuse for it.

Mr. LUNGREN. Do you have any questions that the NSLs are of some value?

Mr. FINE. Yes, I believe they are of value.

Mr. LUNGREN. If we lost them, that would be a loss.

Mr. FINE. I believe they are a valuable investigative tool to counterterrorism and counterintelligence investigations, and that is why it is so troubling.

Mr. LUNGREN. We better fix it so we don't lose a tool that is truly effective.

Mr. FINE. I think they need to fix it.

Mr. LUNGREN. Thank you, Mr. Chairman.

Mr. CONYERS. The gentlelady from Texas, Sheila Jackson Lee.

Ms. JACKSON LEE. Mr. Chairman, again, my appreciation for your continuing effort of establishing transparency in Government.

I welcome both of the witnesses here today and recount just limited history that troubles me as we find ourselves here today. I know the good intentions of the witnesses, but certainly I need not remind you of the era of McCarthyism and certainly that role law enforcement played in that misdirected era of the United States of America.

As a young lawyer, I participated in the investigations into the assassination of Dr. Martin Luther King and John F. Kennedy right here in this Congress; and what was exposed was the extensiveness of the COINTELPRO of Dr. Martin Luther King—wrongheadedness, as far as I am concerned—as relates to the utilization of protecting this country. A civil rights leader who happened to be outspoken against the heinous governmental acts of segregation, and all of a sudden he became a major target of the Federal Bureau of Investigation, with any number of officers, agents, if you will, probing and looking over paperwork that he might have generated.

That smacks, as far as I am concerned, of where we are today, even though, Mr. Inspector General, you have indicated that it has been without malice, without intentions. And we all know that there is a phrase that says, a journey to a certain place is paved on that road with good intentions.

So I am not very happy as to where we are today, because I argued vigorously about the extensive powers that we were giving to the President of the United States out of fear. One thing that the Constitution reminds us and certainly the Founding Fathers, who left a tyrannical society to be free, is that tyranny can get the best of us. Lack of control can get the best of us.

So I ask to the General Counsel of the FBI, did you determine what percentages of those letters that were sent without National Security Letters generated into terrorist responses or terrorist incidences or terrorist prosecutions? I would be interested in that number. Why don't you just answer that yes or no. Do you have the percentage?

Ms. CAPRONI. I do not.

Ms. JACKSON LEE. I would like to get the percentage, frankly.

Ms. CAPRONI. The Director has ordered a special investigation of the whole exigent letter instance. We will brief this Committee when we have the results of that.

Ms. JACKSON LEE. I will join my colleague on the other side of the aisle. How quickly can you get that information? This is about protecting the Constitution and securing the homeland, two very important jurisdictional responsibilities; and I happen to serve on

both Committees, Homeland Security and this. So my question is, how soon can you get those numbers? It makes a real difference to know whether you generated potential terrorist threats that would secure the homeland or whether or not the FBI was on a fishing expedition.

Ms. CAPRONI. Congresswoman, let me assure you that the group was not on a fishing expedition. Having said that, I understand my assurance to this Committee at this point isn't worth a lot. The Inspection Division is conducting the inquiry. They know that they have to proceed quickly, but I regret I can't tell you when they are going to be done. I will make sure that the Director understands that you want it done as quickly as possible.

Ms. JACKSON LEE. Certainly we wish the Director well. We would have wanted to have him appear before this Committee, but we do wish him a speedy recovery.

Ms. CAPRONI. Thank you. I will let him know that.

Ms. JACKSON LEE. Mr. Inspector General, I assume you will say to me that you don't speculate, but let me quickly ask you a question and will you be thinking, the General Counsel, on this question.

The President signed on the PATRIOT Act a signing statement which indicated that he was going to interpret or have the Act interpreted in a manner consistent with the President's constitutional authority to supervise a unitary executive branch to withhold information. Just be thinking about that. I wanted to know, did that give you free ride. That is why I have legislation that indicates that agencies should not be running, I must say, amok because of signing statements.

Mr. Inspector General, what you looked at and you said it has not been intentional—help me out—however, don't you believe there should be restraints put in place and might the PATRIOT Act be entirely too broad to even be a valuable tool that would restrain people in balancing both security and as well balancing civil liberties?

Mr. FINE. I do believe that there need to be controls. I do believe that there needs to be a balance, a balance of effective tools to prevent terrorism, and at the same time effective controls on the use of those tools.

What was most troubling to us was that those controls were not implemented and not followed. I share the concerns expressed by the Members of this Committee, and that is why we did the report.

We were not restricted or limited in what we did, and I know there was a Presidential signing statement, but the Department did cooperate with us. We did provide the information that we had. We provided it in the most unclassified way we could, and the Department actually did unclassify a fair amount of this information so it could be fully aired. We also provided a classified report to this Committee and other Committees describing the additional information. So we did what we could to identify the problems in this program.

Mr. CONYERS. The gentleman from Florida.

Ms. JACKSON LEE. Mr. Chairman, can she answer yes or no on the signing statement? Would you indulge me?

Ms. CAPRONI. The signing statement had absolutely no impact on how we secure letter authority.

Mr. CONYERS. The gentleman from Florida, Mr. Ric Keller.

Mr. KELLER. Thank you, Mr. Chairman.

Ms. Caproni, let me begin with you. If the FBI didn't have National Security Letters as an investigative tool, you could get the same information via prosecutor through a grand jury subpoena or by going before a FISA court and getting a court order, isn't that correct?

Ms. CAPRONI. Yes.

Mr. KELLER. The concern that you have with those two options is you essentially don't have the manpower. I think you said it would sort of sink the system.

Ms. CAPRONI. I was responding to a suggestion that all of these should be obtained via court order. If that were the law, that would create substantial obstacles to our national security program.

Mr. KELLER. That is why you aren't using in all cases the grand jury subpoena or the FISA court orders, because you don't have the manpower power to do that and still do your investigations?

Ms. CAPRONI. I would say it is perhaps slightly more nuanced than that. On grand jury subpoenas, there are cases where we don't have a criminal case open, so a grand jury subpoena is not an option. Further, the whole philosophy of making sure that we are thinking from an intelligence perspective rather than immediately cutting to the chase of a criminal investigation encourages agents to use national security tools versus criminal tools.

Mr. KELLER. Let me follow up, because the challenge we have is getting this in the strike zone. We want you to have this information that you need as an investigative tool, but we want there to be some sort of check on your authority. To use the grand jury subpoena, for example, to get my phone records, I have the ability to move to quash that subpoena and have a judge hear it.

Ms. CAPRONI. Only if someone tells you the subpoena has been served, which is not the typical route of a grand jury subpoena.

Mr. KELLER. Before you went before a FISA court you would have a set of eyes through the FISA court judge looking at it, correct?

Ms. CAPRONI. That is correct.

Mr. KELLER. In terms of using the National Security Letter, let's say you served it on my phone company. The phone company is not necessarily looking out for my personal privacy interests, and so there is not a set of eyes looking at it, at least from an individual perspective.

Ms. CAPRONI. Again, that is the same as with a grand jury subpoena, correct.

Mr. KELLER. So all we have is our Inspector General as a check on the controls to make sure that you are applying it in an appropriate way.

Ms. CAPRONI. I think this report has told us we internally have to do a far better job at making sure that we are maintaining internal controls over the use of this tool. I fully expect Mr. Fine to come back to visit us in future years and will dutifully take us to task if we have not accomplished that.

Mr. KELLER. Mr. Fine, imagine a housewife in Orlando, Florida. She does absolutely nothing relevant to terrorism or espionage, never met or spoken to a terrorist or spy. Based on your investigation, does she have any reason to worry about National Security Letters violating her privacy by looking at her phone records, bank records or Internet search records?

Mr. FINE. I think that there are times when the FBI looks for telephone records of potential terrorists and looks to see who they have contacted or been in contact with. Could be advertent, could be intentional contact, could be inadvertent contact. As a result of that contact, there can be efforts to look and see what telephone numbers have been called.

Now, if they had no contact whatsoever with the subject of a potential terrorist investigation, it is less likely that the records would be obtained here.

Mr. KELLER. In framing my question, I said, no contact, either written or spoken. So let me ask you, based on your investigation, were there any situations where you saw National Security Letters being used when there was no relevance whatsoever to international terrorism or espionage?

Mr. FINE. We couldn't in our review look at all the investigative case files and say there was an adequate predicate. There wasn't. We looked at how they were used and whether on their face they were improper. So it is impossible for us to say that the relevancy standard was met.

One thing we did find and I would note, this is that, in many cases, the counsel of the FBI field offices, either the Chief Division Counsel or Assistant Counsel, did not aggressively and independently look for that. And they are the ones who should be checking on that, they are the ones who need to ensure there is adequate predicate for this investigation. And we saw in many cases that that didn't happen that they acceded to the wishes or the arguments of the case agents or special agents in charge without independently and aggressively looking at that.

Mr. KELLER. One final question. Can you give us an example to help make your case, if you have one, as to what is a scenario where a National Security Letter is your best investigative tool because, for whatever reason, a grand jury subpoena or a FISA court order is insufficient?

Ms. CAPRONI. Any time I would say that they were at the very beginning of an investigation; say, for example, after the London bombing when the British authorities provided us with telephone numbers of the British bombers. So we were looking to see if we have anyone in the United States that had telephone contact with the London bombers. In my view, the appropriate way to pursue that investigation is via National Security Letter.

Mr. KELLER. Because you wouldn't have time under the other options?

Ms. CAPRONI. We wanted to know that very quickly; and, again, I think the American people would want us to know very quickly after the London bombings took place whether we had any cells or groups of people tightly related to the London bombers. So we needed to move very quickly; and, in fact, the investigators did move very quickly on that to figure how out who here was con-

nected to there and was it an innocuous connection or a dangerous connection.

Mr. KELLER. My time has expired.

Mr. CONYERS. The distinguished gentlelady from Los Angeles, California, Maxine Waters.

Ms. WATERS. Thank you very much, Mr. Chairman.

May I ask, were these witnesses sworn?

Mr. CONYERS. They were not.

Ms. WATERS. May I respectfully request that they be sworn in?

Mr. CONYERS. Too late.

Ms. WATERS. Then, Mr. Chairman, I suppose we are going to have to rely upon them, particularly the General Counsel, continuing to tell us that they are acting within the law.

I shall proceed with my questions.

Mr. CONYERS. If the gentlelady will yield, false testimony before this Committee can constitute a violation in and of itself, a misstatement, any deliberate misstatements.

Ms. WATERS. Well, I would have preferred that they be under oath, but—however, the Chair has made that decision; and I shall proceed.

Let me just ask about the use of these exigent letters. As I understand it, these letters are used basically to get around having to get the NSL letters; is that right, Mr. Fine?

Mr. FINE. These letters were used in advance of or in lieu of National Security Letters, that is right.

Ms. WATERS. There was information collected as a result of these letters, particularly the operation I believe that was set up with the contract with the three telephone companies or telecommunications companies; is that correct?

Mr. FINE. Well, there were contracts with the telephone companies so that they would provide information to the FBI on an expedited basis.

Ms. WATERS. Ms. Caproni, do you still have contracts with those telephone companies, any other telephone companies, or any other private businesses to supply you information in the manner that those companies did?

Ms. CAPRONI. We continue to have contracts with the telephone carriers that obligate us to provide them with appropriate process to get records.

I can't answer the balance of your question. I don't know if we have other contracts with other private parties. The telephone companies it made sense, because of the volume of our request.

Ms. WATERS. How much are the taxpayers paying the telephone companies, that they pay to provide them services to spy on us?

Ms. CAPRONI. I don't know what the dollar value of the contracts are.

Ms. WATERS. You have no idea?

Ms. CAPRONI. I actually don't.

Ms. WATERS. You have never heard any discussion about it?

Ms. CAPRONI. I am sorry, I don't. I just don't know the amount.

Ms. WATERS. Information was collected on millions of Americans using this as a tool. Now that you know that they are were innocent, they probably should not have been under investigation. Has all of this information been purged and gotten rid of?

Ms. CAPRONI. We did not collect records on millions of Americans?

Ms. WATERS. How did it work then?

Ms. CAPRONI. The exigent letters were provided to the carriers, which promised future process. That future process, unfortunately, was not always promptly provided.

Ms. WATERS. What did they do?

Ms. CAPRONI. Who do?

Ms. WATERS. The companies. How did they mine the information and did they mine information of innocent people?

Ms. CAPRONI. The carriers provided us with toll billing information, which was then placed into our databases. There is no connection between their databases and our databases. The information comes out electronically and moves into ours.

Again, we are talking about—I believe the number of numbers at issue, according to the Inspector General, is somewhere in the neighborhood of 3,000. It is my belief, though—again, we will have to wait and see what the special inspection finds—that all of those numbers were tied to authorized investigations. To the extent any were not, the records will be removed from our databases and destroyed.

Ms. WATERS. When will they be removed? How long will it take?

Ms. CAPRONI. Again, I am anticipating that that special inspection will take a couple of weeks at least, but probably—I just actually don't want to speculate.

Ms. WATERS. Didn't you have a court order relative to your contracts with these telephone companies?

Ms. CAPRONI. No, ma'am.

Ms. WATERS. Was there a court decision relative to the manner in which information was obtained?

Ms. CAPRONI. The information was obtained from the carriers pursuant to—it was supposed to be obtained pursuant to the laws of ACBA.

Ms. WATERS. But they were not.

Ms. CAPRONI. Again, as Mr. Fine has indicated, there were these exigent letters that were used. What we are trying very hard to do is to unravel and to make sure that we do not have the records of anyone as to which there was not—it wasn't relevant to an authorized investigation.

Ms. WATERS. How long have you been trying to do this?

Ms. CAPRONI. We began the process with them last fall and we are—we within OGC are to the point that if they cannot demonstrate to our satisfaction very quickly, then any of those records have to be removed from the database and destroyed.

Ms. WATERS. Certificate letters, are you still issuing certificate letters?

Ms. CAPRONI. No.

Ms. WATERS. When did you stop?

Ms. CAPRONI. Shortly after OGC learned about them, that process was stopped. We entered into discussions with the Fed over whether—Federal Reserve Bank in terms of whether or not it required a National Security Letter. There was some back and forth between lawyers, that the decision was made that they would prefer a National Security Letter, so——

Ms. WATERS. So you collected information using these certificate letters. Has that information been destroyed?

Ms. CAPRONI. No.

Ms. WATERS. When are you going to do it?

Ms. CAPRONI. I don't believe we are going to do it.

Ms. WATERS. Why are you going to keep information that was improperly collected on financial records of innocent people? Why would you keep it?

Ms. CAPRONI. One, they are not innocent people; and two, it wasn't improperly collected. The Federal Reserve Bank is not directly covered by the right to financial privacy. They can ask for a National Security Letter, which they now have done, and because——

Ms. WATERS. Why did you stop using certificate letters if they were legal and proper?

Ms. CAPRONI. Because we thought the better process was a National Security Letter, and the Fed asked us to provide National Security Letters.

Ms. WATERS. How have you determined whether or not the information you collected was on individuals who were suspicious, guilty, had committed a crime? How do you determine whether or not these people are innocent and the information should be destroyed?

Mr. CONYERS. The gentlelady's time has expired. Please answer the question.

Ms. CAPRONI. Certainly. The issue is whether the information is relevant to an investigation. There are times when we gather information that is relevant to an investigation but it turns out that the person was not engaged, for example, in terrorist financing. We don't then destroy the information, though the investigation is closed. So it is much like any other information that is gathered during the course of an investigation.

The issue of whether that policy will continue is a matter that is under discussion by a group that is being chaired by the DNI in terms of whether we should or we should not continue to retain information that is gathered via National Security Letters after the investigation is closed.

Mr. CONYERS. The gentleman from Virginia, Mr. J. Randy Forbes.

Mr. FORBES. Thank you, Mr. Chairman.

Mr. Chairman, I hope I can emulate your very calm manner of handling this Committee; and I just want to tell the witnesses what I said at the beginning—I want to thank you both for being here. We know you have a tough job, and we appreciate you coming in here and answering our questions today.

I have listened to the Committee as we have gone through this process, and we have had testimony from the Washington Post, we have had testimony from members of the audience, testimony from Members of this Committee. You are the only witnesses we have here.

I think that you get the message, both of you, you had it when you came in here, that no one on this Committee condones any of these lapses or feels that it is not urgent that they be corrected and corrected as quickly as possible. We are also grateful that this

Committee requested this audit. Because, Mr. Fine, through your good work, we were able to find out what these problems were so that we can correct them.

The other thing, Ms. Caproni, you have been asked to take a lot of messages back to the FBI, all of which are good and valid messages. But another one I want to ask you to take back today is that, although the FBI messed up in handling the NSLs, I want you to take a message back to those agents in the field, who I know are working around the clock; they are away from their families a lot of the time, and thank them for not messing up on what Mr. Fine said was one of their key missions and that was to detect and deter terrorism and espionage in this country. Because if you had messed up on that one, we would have a lot more people in this room and a much harsher hearing than we are having today.

The other question I would like to ask either of you to respond to: Do either of you have any evidence today that anyone in a supervisory position gave instructions, either expressly or impliedly, to any person under his or her supervision to misuse the NSLs?

Ms. CAPRONI. Not to my knowledge.

Mr. FORBES. Mr. Fine.

Mr. FINE. We did not find that evidence. We did not find that there was an intent by people who knew they were misusing it to misuse it. So, no.

On the other hand, we did not do a thorough review of what people up and down the line knew and did, so we reported what we found.

Mr. FORBES. That is being conducted, as I understand it, now, is that correct?

Ms. CAPRONI. Correct.

Mr. FORBES. And if you find that information you will present that back to the Committee, correct?

Ms. CAPRONI. Absolutely.

Mr. FORBES. The second question for either of you: Is there any evidence that any member of the FBI or the Justice Department provided any information either orally or in writing to this Committee or to Congress which they knew to be inaccurate or false?

Ms. CAPRONI. Not to my knowledge.

Mr. FORBES. Mr. Fine, you don't have any?

Mr. FINE. I don't have that information, no.

Mr. FORBES. Just the balance that we have talked about, we know the harm that comes from violation of privacy interests of our citizens, that is huge. But I wish you would go back—and, again, just take a minute—and talk about what Mr. Fine has put in here about—says: These tools are indispensable to the FBI's mission to detect and deter terrorism and espionage.

We know there has been a lot on your plate since 9/11 and you have had to do that. Can you tell us, with as much specificity as you can, exactly how these NSL letters have helped to do and accomplish that mission?

Ms. CAPRONI. Again, National Security Letters provide the basic building blocks of an investigation. Starting with phone records, phone records are critical to the counterterrorism agents to figuring out who was connected to whom; and that permits us to trace foreign terror acts that have occurred, obviously, since 9/11 and trace

them in to individuals who are in the United States and to determine whether those individuals are up to no good or, in fact, it is just an innocent connection. But for National Security Letters, I don't know how we would do that.

They have also been absolutely indispensable in the area of terrorist financing. We have done a tremendous amount of work getting bank records on individuals we believe are funneling money to foreign terrorist organizations overseas. Again, without National Security Letters, could we go through a FISA order? We probably could, but we certainly couldn't do that very efficiently. So a National Security Letter is an efficient way for us to get the basic building blocks of an investigation.

Mr. FORBES. Have they stopped any terrorist attacks that you know of that could have possibly happened in the United States? You may not have that information.

Ms. CAPRONI. I am sorry, I don't.

Mr. FORBES. Thank you both.

Mr. Chairman, I yield back the balance of my time.

Mr. CONYERS. I thank the gentleman.

The Chair recognizes Stephen Cohen, the gentleman from Memphis, Tennessee.

Mr. COHEN. Thank you, Mr. Chairman. Stephen, yes. You can call me Stephen.

Mr. CONYERS. Stephen.

Mr. COHEN. Thank you, sir.

Mr. Fine, did you do any study of the people whose records were looked at illegally for any similarity in demographics?

Mr. FINE. No. We looked at whether they were U.S. persons or non-U.S. persons, but within those persons we did not look at the demographics of those individuals.

Mr. COHEN. Ms. Caproni said they were all with investigations that were ongoing. Did you find that to be true, also?

Mr. FINE. We could not verify that they were all connected to an ongoing investigation. I know the FBI is trying to do that now. But as part of our audit we could not do that, all that.

Mr. COHEN. Do you think it might be a good idea to look at those people to see if there are any demographic consistencies, if there is a group of the American public that might be looked at in a closer manner than others and that might——

Mr. FINE. It is possible. That would be quite an undertaking, and one has to realize a lot are not on individuals but are on telephone numbers. There are certainly consumer credit reports and other things that do relate to individuals. So that kind of review is possible but incredibly intensive and requires additional resources while we are trying to comply with this Committee's and the Congress's directive to do a review of the use of them in 2006 according to the guidelines that were set out here.

Mr. COHEN. Thank you.

Ms. Caproni, you said that these were all tied to investigations, is that correct?

Ms. CAPRONI. I said I believe that they are all tied to investigations, and that is what we are trying to work through with that unit now.

Mr. COHEN. If you find that they are not tied to investigations, could you make a report to this Committee of who those individuals were and why they were—their records were sought when they weren't tied to investigations?

Ms. CAPRONI. Yes, we will provide this Committee with what we find through the course of that special inspection.

If I could just say, though, so there is no misunderstanding, the unit at issue typically gets simply a telephone number. So they don't know—that is part of with what they are charged of finding out, is who belongs to this telephone number, what are the toll billings, records for this number. So the name of the person associated with the phone number is typically not part of what CAU does.

And for the exigent letters, to my knowledge—again, the special inspection will reveal much more in terms of the ins and outs of what they were doing—they were working off of telephone numbers and not off of names.

Mr. COHEN. In the report, it says that some of these violations demonstrated FBI agents' confusion and unfamiliarity with the constraints on National Security Letter authorities. Other violations demonstrated inadequate supervision over the usage of these authorities.

This is from Mr. Fine's statement.

Ms. Caproni, do you think that these are maybe indices of a systemic problem with the FBI, where the agents have confusion and unfamiliarity with other policies and other laws? And, if so, are you doing something about it?

Ms. CAPRONI. Congressman, that is exactly what I am concerned about.

In the discussions that we have had—and I can tell you that we have had a lot of soul searching at the FBI since then. We got an F report card, and we are just not used to that. So we have had a lot of discussions about this.

One concern is, are we—most of the agents grew up—the agents my age at the FBI all grew up as criminal agents in a system which is transparent, which if they mess up during the course of an investigation they are going to be cross-examined, have a Federal district judge yelling at them. The national security side occurs largely without that level of transparency.

Our concern is and what this report has shown us is that we have simply got to do a better job making sure that, although the actions that are taken in national security investigations are typically taken in secret and they don't have the transparency of the criminal justice system, that that imposes upon us a far higher obligation to make sure that we have a vigorous compliance system, that we have in place the training that is necessary, that we restrain agents, that when agents are working in this area we make sure they know.

Mr. COHEN. I think that is what we need. I appreciate your candor.

There is some signage in the Capitol and one is a statement by Brandeis, something to the effect that the greatest threats to liberty come from insidious men of zeal, well-meaning but without knowledge or understanding.

I think that you will find that if our agents, our FBI agents, even though well-meaning and zealous, don't know what they are doing, that it is a threat to people having faith in the whole system. I hope you will correct that. I feel confident you will.

Ms. CAPRONI. You are absolutely correct. We will.

Mr. COHEN. Thank you.

Mr. CONYERS. I thank the gentleman, Steve Cohen.

The Chair recognizes now the gentleman from Virginia, Bob Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman, and thank you for holding this hearing.

Ms. Caproni and Mr. Fine, thank you for your testimony today. These are very serious concerns, and we appreciate your helping us understand how they occurred, why they occurred, and what is being done to correct them.

I have several questions I would like to ask, starting with you, Ms. Caproni.

In Mr. Fine's report on page 8, paragraph 3, he notes, "In addition, we found that the FBI had no policy requiring the retention of signed copies of National Security Letters. As a result, they were unable to conduct a comprehensive audit."

Can you explain why something as important and serious as a National Security Letter would not have a signed copy retained in the records of the Bureau?

Ms. CAPRONI. I can say that there were different processes in different field offices; but, no, I cannot. I mean, there is just no reason why there was not a policy that said you have to keep a copy of the signed copy.

What we keep, which is typical of how our records are, is the carbon copy, in essence, which is typically initialed.

But, no, in the world of Xerox machines, there is no reason why we had not told people to hang on to a signed copy.

Mr. GOODLATTE. Mr. Fine, did you draw any further conclusions from that? Do you know why they were not retained?

Mr. FINE. They were not retained because there was not a clear policy that was enforced.

Mr. GOODLATTE. No ulterior motive that you know of?

Mr. FINE. I do not believe there was an ulterior motive, but this was an example of an incredibly sloppy practice that was unacceptable.

Mr. GOODLATTE. I agree.

Let me ask you, when did you first learn of the problem with the FBI's improper use of the exigent letters?

Mr. FINE. Well, we began our audit, as required by the PATRIOT Reauthorization Act, around the beginning of 2006. As you can see from this report, there are a lot of issues, and we did interviews and document requests and field files.

I think sort of the first indications where we learn about it were in the spring or summer of last year, where we had to work through those issues.

Mr. GOODLATTE. And who did you learn that from?

Mr. FINE. We learned it from, I believe, people in the Office of General Counsel, the National Security Law Branch of the FBI, about these issues. I think they are the first people we learned it

from, as well as from the review of documents and e-mails and things like that.

Mr. GOODLATTE. And what steps have you taken to ensure that the practice was stopped?

Mr. FINE. The steps we have taken are to inform the FBI about the unacceptability of this practice, to note it, to report it, to let the people who are in charge of the FBI and the General Counsel's Office know about it, and to make a recommendation that it does stop.

Mr. GOODLATTE. When did you make that recommendation?

Mr. FINE. I think we made the recommendation when our report was issued to the FBI in draft; and I think that was in either December or January of this year. It was December of last year or January of this year.

Mr. GOODLATTE. Ms. Caproni, has that practice been stopped?

Ms. CAPRONI. Yes.

Mr. GOODLATTE. What steps have you taken to ensure that it does not persist in any of the offices of the FBI?

Ms. CAPRONI. Well, first, we are trying to find out whether it did happen in any office other than the unit at headquarters, and we should know that answer probably by the end of this week or sometime next week.

The second thing is that the practice of providing a letter with a promise of future legal process has been banned. And, again, we are also developing a vigorous compliance program to make sure that we do not simply make the rule, but we actually have in place some kind of process to make sure that the rules are being followed.

Mr. GOODLATTE. Current law authorizes a full credit report request for only counterterrorism investigations. The Inspector General discovered two instances in the same field office of a full credit report request under counterintelligence investigations.

How is this being corrected?

Ms. CAPRONI. This is being corrected by—the deputy director ordered a full audit of every counterintelligence file that has been opened since January 1, 2002. This authority went into effect in the PATRIOT Act. So, realistically, we think the earliest one that could have been issued would have been in 2002.

So they have to review every file since then in which a Fair Credit Reporting Act NSL was issued and find out if they have any full credit reports. If they do, they need to remove them from their files and report it as a potential IOB violation. Those will, in turn, be reported on to the IOB.

Mr. GOODLATTE. One last question.

In at least one instance, a National Security Letter issued under the Electronic Communications Privacy Act was determined by the Inspector General to be seeking content.

How was this remedied, and what steps do your field agents take to delineate between content and transaction information?

Ms. CAPRONI. In that case, there was no need to remedy it because the Internet service provider refused to provide us with any records, so we actually did not have an overcollection.

Mr. GOODLATTE. Have you remedied the request? I mean, they should not be asking for that.

This was a big issue when we wrote the PATRIOT Act, and it was the subject of a great deal of discussion with the Administration about making sure that we had a clear line between what could be requested and what could not be requested.

Ms. CAPRONI. The statute defining electronic communications transaction records actually does not define the term, and there had traditionally been the debate that says that we will leave up to the ISP what is content and what is not.

We think that is a trap for the unwary. It is bad for our agents in that we do better with bright lines. And so OGC will establish—we are in the process of making sure that we have a list that makes sense of what is content and what is not.

In the abstract, that seems like a very clear line; in practice, it is not. There are some difficult issues because some of the answers revolve around how the ISP keeps their records.

So we are working on it. My anticipation is that, within the next week or two, we will have out to the field these records you can seek, these records you cannot seek, and it will be a very bright line.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. CONYERS. The gentleman from Georgia, Mr. Hank Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman.

In these reports that I have read, it indicates that there were three phone companies that the FBI, particularly the FBI Communications Analysis Unit, the CAU, contracted with three telephone companies between May of 2003 and March of 2004. Who were those telephone companies?

Ms. CAPRONI. The telephone companies were AT&T, Verizon and MCI, which has now been acquired by Verizon.

Mr. JOHNSON. Now, are those contracts still in force at this time?

Ms. CAPRONI. Yes, they are.

Mr. JOHNSON. And are there any other phone companies that are contracted with the FBI through the Communications Analysis Unit or any other unit of the FBI?

Ms. CAPRONI. Not through the Communications Analysis Unit; broader than that, I do not know. We may have contract—not for this sort of information. We may have other contracts with phone companies, but not like this.

Mr. JOHNSON. And nobody put a gun to these telephone companies' heads and made them sign the contracts, did they?

Ms. CAPRONI. No.

Mr. JOHNSON. They were just simply agreements with the FBI and with the phone company?

Ms. CAPRONI. Correct. From our perspective, because these originated—given the volume of our requests, that this permitted us to get our records very quickly.

Mr. JOHNSON. Well, I understand.

Then the phone companies received compensation for engaging in this contract with the FBI; is that correct?

Ms. CAPRONI. That is correct.

Mr. JOHNSON. And this compensation, was it merely for expenses or was there profit involved, or you have no way of knowing?

Ms. CAPRONI. I do not know.

Mr. JOHNSON. Really, you do not really care as long as you get the information, correct?

Ms. CAPRONI. Again, from our perspective, the goal was to get the information in a form that is readily usable for us so that we do not have—some phone companies give us paper records. That requires a lot of data.

Mr. JOHNSON. Okay. All right. I understand.

Earlier in your testimony, ma'am, you stated that the phone companies were responsible for a lot of the errors that are cited in the compliance with the National Security Letters.

Ms. CAPRONI. We do see third-party errors, correct.

Mr. JOHNSON. You saw a substantial number, and so you are placing upon the phone company the obligation to properly document whether or not there has been a follow-up with an exigent letter?

Ms. CAPRONI. Oh, no, sir. They are two separate things. I do not excuse our lack of recordkeeping in connection with the exigent letters. They did keep the records, which was fortunate.

Mr. JOHNSON. And it is important to note, Mr. Fine, that your analysis of the FBI's compliance with the PATRIOT Act found that there were woefully inadequate mechanisms for the collection of data on these National Security Letters. In other words, the recordkeeping by the FBI was woefully inadequate as far as the issuance and follow-up on these National Security Letters and also the exigent letters; isn't that correct?

Mr. FINE. We did find serious and widespread misuse and inadequate recordkeeping, absolutely.

Mr. JOHNSON. Do you have any idea, Mr. Fine, how much the telecommunications companies were paid for their so-called "contract" with the Government?

Mr. FINE. I do not know, no.

Mr. JOHNSON. All right.

Can you, Ms. Caproni, provide my office with that information, along with copies of the contracts between the CAU and the phone companies?

Ms. CAPRONI. I have great confidence that we are going to get a number of questions for the record after this, and I am assuming that will be one of them, and we will respond appropriately.

Mr. JOHNSON. Will it take a subpoena for us to get that information?

Ms. CAPRONI. I do not believe so. I do not know what is in the contract, so I do not know if there are any sensitive issues.

Mr. JOHNSON. Will you provide it to my office?

Ms. CAPRONI. Again, we will respond to questions for the record as they come in.

Mr. JOHNSON. All right.

Why, if the NSLs are the FBI's bread-and-butter investigative technique, could the Inspector General only identify one terrorism prosecution out of the 143,074 people whose investigatory information was obtained?

Ms. CAPRONI. Again, Mr. Fine can explain his methodology, but I think the issue and the difficulty of that question is that because there was no congressional—because we were not legally obligated to tag the data, tracing it through is difficult.

Mr. JOHNSON. So 1 out of 143,000.

How does that equate to being the bread-and-butter investigative technique for uncovering terrorism by the FBI?

Ms. CAPRONI. Again, we disagree that in only one case did NSL data contribute to a criminal prosecution.

Mr. JOHNSON. But would you say more than 10 or less than 10?

Ms. CAPRONI. I do not know. It is my belief that virtually every counterterrorism case that began in its normal course of affairs is likely to have a National Security Letter used sometime during it.

Mr. JOHNSON. And it is also——

Mr. CONYERS. Your time has expired.

Mr. JOHNSON. Thank you.

Mr. CONYERS. Mr. Johnson, any records that you request will come to the Committee, and then you will be advised.

The Chair is pleased now to recognize the gentleman from Florida, Mr. Tom Feeney.

Mr. FEENEY. Thank you very much, Mr. Chairman.

Earlier, Mr. Smith alluded to your illustrious basketball career. I went to the same high school as Mr. Fine. He graduated a few years before me, and I wish I had had a jump shot like Mr. Fine did, but not nearly so much as I wish I would have been able to hit a fast ball like Mr. Reggie Jackson, who graduated a few years before Mr. Fine did.

But we thank you for your work. By the way, none of us is the most famous graduate because Benjamin Netanyahu, the former Prime Minister of Israel, is. I had to get that plug in.

We are very grateful for your work here, because a lot of us are supporters of the PATRIOT Act, but only with some serious restrictions. And I guess the first question I want to ask you—and I want to remind people that it was the reauthorization of the PATRIOT Act that actually required the report that you have just completed; is that right?

Mr. FINE. Yes.

Mr. FEENEY. And I hope that not just your report but the tenor of the questions from supporters of the PATRIOT Act, as well as the critics, is being listened to very carefully in the Justice Department and in the FBI.

We have got to get this balance correct; and nothing could be more critical because some of the most unthoughtful critics of the PATRIOT Act candidly will be the first ones—when there is another 9/11 and when we do not get the information accurately ahead of time to stop, maybe not 3,000 or 4,000 people, but 300,000 or 400,000 people, they will be the first ones jumping on the Administration, the Justice Department and the FBI for not doing its job.

But those of us trying to strike a thoughtful balance between civil liberties and the need to protect America from this new threat are very, very concerned about what we have heard, and if the FBI does not take this to heart, we will correct the problem.

I do not think anybody could have said it better than Jim Sensenbrenner, who, again, is a supporter of the PATRIOT Act, who said that the overreaching that is apparent here within the FBI is going to erode support, if it has not already, for very important national security initiatives. And I would hope that everybody down

at Justice is listening because these are the supporters, people like Lungren, Feeney and Sensenbrenner, who are telling you this is not right, that it cannot continue.

Mr. Fine, do you have an opinion as to whether or not the serious problems that you have discovered in initial compliance with the PATRIOT Act are largely because of ambiguities or poorly structured legislation? Is it statutory language that is the problem, largely, here; or is it abuses within the FBI and compliance?

Mr. FINE. I do not think it was the statutory language that was ambiguous. I think it was the execution of the policy by the FBI that was woefully inadequate.

Mr. FEENEY. Just to follow up, can you identify or do your report and investigation lead you to conclude that there are any important statutory improvements we can make?

I realize it is not your typical arena to give us advice, but are there any specific pieces of advice that you would give the Congress in terms of oversight or statutory reforms here?

Mr. FINE. Well, you are correct, it is not my arena to do that. What I try to do is present the facts to this Committee and to Congress and let the facts lead this Committee and Congress to do what they believe is appropriate.

There is one section of the report that does talk about an ambiguity in the meaning of toll billing records. I think there ought to be something done about that, because that was a concern of what that meant, and it should be clarified.

I do think——

Mr. FEENEY. Could the AG do that, by opinion?

Mr. FINE. I do not think so. It has to be done by Congress.

I do think that the Committee does need to strike a balance and to sort of balance the need for protections and controls over civil liberties with the need for tools to prevent and detect and deter terrorism. And that is the difficulty in this task, and that is the real concern that we have about how the FBI implemented this.

Mr. FEENEY. You said you sampled 77 case files, the report indicates. How many case files are there all together, roughly?

Mr. FINE. That I could not tell you.

Mr. FEENEY. Do you believe that the 8,850 failed reportings are systemic and that, if you would extrapolate, we would probably see that elsewhere?

Mr. FINE. I do believe that the files we looked at were a fair sample and that there is no reason to believe that it was skewed or disproportionate. We did not cherry-pick them.

Mr. FEENEY. Do you have any reason to believe that there were more abuses in the 8,850 requests that were not properly reported? Is it any more likely for there to be abuses of civil liberties or of the law or of the AG's rules than the requests that were properly recorded?

Mr. FINE. Well, we do not know how many requests were not recorded in the FBI's database. There were problems with the database structurally so that things were not in there. There were delays in entering in the database, so Congress did not get the information, and when we looked at the files, there were NSLs that were in the files that did not go into the database.

Approximately—I think it was 17 percent of the ones we found were not in the database. Now, that is a significant number; and now—I know the FBI is trying to find them in the database as we speak, but we have no confidence in the accuracy of that database.

Mr. FEENEY. Finally, if I could, Mr. Chairman.

Ms. Caproni, you alluded to the culture of the FBI, which traditionally, I find, is a crime-fighting institution. Some people have called for an N15 type of intelligence agency with a different culture, and it might be interesting that you take back the interest that some of us in Congress have, that if the FBI cannot change its culture or have a separate culture for intelligence than it has had traditionally, we very much need a different type of institution to get intelligence right, to protect this country on a day-to-day basis.

Ms. CAPRONI. Again, I believe that we can do this. We are going to do this. We can get this right. We are going to get it right.

Mr. FEENEY. Mr. Chairman, I yield back the balance of my time.

Mr. CONYERS. Thank you. There was not any left.

Mr. FEENEY. That is why I did it.

Mr. CONYERS. I see.

Okay, we are now going to recognize the gentleman from California, Mr. Adam Schiff.

Mr. SCHIFF. Thank you, Mr. Chairman.

Inspector General Fine, you have said that you did not find that any of the violations were deliberate or intentional, and yet, you also report the issuance of blanket NSLs, which, to me, appear to be an effort to cover up what was recognized to be a flawed issuance of these exigent letters.

Given that NSL letters are supposed to be case-specific, the NSLs were a blanket violation of the law, weren't they? How can they be described as unintentional or anything but deliberate?

Mr. FINE. I think what you are referring to, Congressman Schiff, is the issuance of what we have heard about of blanket NSLs in 2006. We have not reviewed 2006 yet. We reviewed 2003 to 2005. We have heard about this. It is past the review period, and we are concerned about it, and we will look at that.

Mr. SCHIFF. Well, Ms. Caproni, in your briefing on the Hill last week, you acknowledged that when agents realized that they had been issuing these letters, these exigent letters, saying that subpoenas were forthcoming when they were never forthcoming, that blanket NSLs were issued as a way of basically trying to clear up or cover up or, in other words, make up for the failure to use correct processes in the past.

Assuming those are the facts, Inspector, doesn't that show a level of deliberateness and intention that far exceeds what you have described in your report?

Mr. FINE. It certainly shows us concern of what were they thinking. They clearly were not following the procedures. They clearly were not providing NSLs in advance or even, quite reasonably, soon thereafter; and it did give us concern.

And there were a lot of people who did this. It was done as a sort of routine practice which is, in our view, completely unacceptable. But I think it is important for the FBI to look at this and to inter-

view these people and find out what happened up and down the line. And we will be looking at it, as well, in 2006.

Mr. SCHIFF. Well, even as to the false statements themselves, in these exigent letters that said that subpoenas were forthcoming when they were not, let me ask you, Ms. Caproni, if a local cop in the city of Burbank in my district wrote letters to the phone company, or went out and served letters on the phone company, saying that Federal grand jury subpoenas would be forthcoming, because that local cop wanted to get information that maybe he could not get another way, or could not get as quickly another way, and you learned about this practice, that cop would be under Federal investigation, wouldn't he?

Ms. CAPRONI. Congressman, I really do not know that. I do not think you have given me enough facts to say whether that would or would not be the case.

Mr. SCHIFF. Well, a local police officer acting under the color of Federal law, demanding records, claiming a Federal process that is nonexistent, that would not be an issue for a Federal investigation?

Ms. CAPRONI. It would certainly be troubling, much as the practices that were taking place in the CAU unit are troubling.

Mr. SCHIFF. Well, you know, having worked in the Corruption Section of the U.S. Attorney's Office in L.A., I can tell you it would be more than troubling. You would have FBI agents assigned to investigate that local cop.

It does not seem to me to be any different to have FBI agents giving telecommunications providers letters saying that subpoenas are forthcoming when they are not.

When did your office discover that these old New York form letters were being used to get information?

Ms. CAPRONI. Sometime in 2006.

Mr. SCHIFF. You know, there is a report in The Washington Post that indicates the head of the Communications Analysis Unit, the same unit that drafted most of these letters, warned superiors about the problems in early 2005.

Do you know anything about that?

Ms. CAPRONI. I know what I have read in the paper, and I know that the Inspection Division is going to do a full inspection of this to see what exactly the unit chief said.

Mr. SCHIFF. Well, I am asking you to go beyond what you have read in the paper, and we all know what the IG is going to do.

When did you first learn about the fact that the head of the unit that was drafting these letters had warned superiors—do you know who those superiors are?

Ms. CAPRONI. I do not know who he says he warned.

Mr. SCHIFF. Were you warned by him?

Ms. CAPRONI. No.

Mr. SCHIFF. Do you know if anybody in your office was warned by him?

Ms. CAPRONI. I am not sure that I even necessarily agree that there was a warning. I know that there were—and I knew generally that there were what I understood to be bureaucratic issues within that unit. That did not include——

Mr. SCHIFF. You keep on describing these bureaucratic issues. I find an interesting kind of mix of an acceptance of responsibility

in your statement and a denial of responsibility. You seem to accept responsibility for mistakes others have made, but acknowledge very little responsibility on behalf of the office you run.

It is primarily your office that is intended to advise the agents about how to comply with the law, particularly in an area where the courts are not scrutinizing it, as you pointed out, in a process that lacks transparency.

Isn't that fundamentally the job of your office?

Ms. CAPRONI. That is fundamentally the job of my office.

Mr. CONYERS. The time of the gentleman has expired.

The Chair recognizes Louie Gohmert of Texas.

Mr. GOHMERT. Thank you, Mr. Chairman. I appreciate that.

I am very pleased that when we renewed the PATRIOT Act, we did insert the provision that would require this Inspector General report so that we could find out this information that is so very important.

In your report, your indications, Mr. Fine, were that the FBI did not provide adequate guidance, adequate controls, or adequate training on the use of these sensitive authorities; and that oversight was inconsistent and insufficient.

Ms. Caproni, as I understood Director Mueller to say last week, he took responsibility for the lack of training and experience, and that troubled me a great deal. You had indicated earlier that people of, I guess, our generation and especially those in the FBI had grown up with accountability, knowing they could be cross-examined. And yet, it seems that the overzealousness that Mr. Cohen spoke of often is found in maybe new agents who do not have the time on the ground, the experience.

Wouldn't you agree that is sometimes found in newer agents who lack the training and experience?

Ms. CAPRONI. I do not know in this case if this is an issue of young agents versus old agents. I just do not know the answer to that.

Mr. GOHMERT. Well, are you familiar with the new personnel policy that this Director instituted in the FBI that is affectionately, or unaffectionately, called the "up or out policy"?

Ms. CAPRONI. Yes, sir, I am.

Mr. GOHMERT. You know, I appreciate the Director last week saying that we welcome more oversight; I appreciate your openness in that regard. But just in my couple years of being in Congress, it seems to me that the FBI, at the very top at least, was not interested in oversight and was set on intimidating anybody who really wanted to pursue that.

I know we have one Member of Congress, a former FBI agent, who had indicated to me that—because many of us who are very familiar with many FBI agents, we have been hearing that this policy was causing the FBI to lose some of their best supervisors.

The policy is basically—as I understand it, once you have been a supervisor for 5 years, then you either have to move up to Washington or move out, that you cannot be a supervisor; and that we have lost many of our best supervisors, and we just put new, inexperienced people in supervisory capacities. And this was something that Mike Rogers, a former FBI agent and a Member of Congress, wanted to talk to someone about; and when he finally was able to

get somebody to agree, in a supervisory position, he goes back to his office and his whole office staff is out in the hall because the FBI has come over and done a sweep of his office that was really unnecessary, and it seemed to be more about intimidation.

One of the most outspoken critics of the FBI in the last couple of years has been Curt Weldon, and we know that, back in September-October, the FBI announced, well, gee, he is under investigation just at a perfect time to get him defeated. And so it seems, when we find out that there are all of these 143,000 letters that were inappropriately requested and that, gee, somebody asked tough questions of the FBI personnel and they may very well be the 143,000 and first letter in the next batch inquiring about their own records, that there has not been this desire for oversight, but there has been quite some intimidation.

So I am curious, has there been any revisiting of this up-or-out policy to get rid of the best trained and experienced supervisors since this lack of training and experience and inadequate guidance and controls have come to light?

Ms. CAPRONI. Congressman, the period of time covered by Mr. Fine was at a period of time when those supervisors would have still been in place. What we have seen, actually, is that the 5-year up-or-out has encouraged people to bid for and seek promotion to higher positions, which has been a net positive.

Now, I know that you have an interest in this, and I know that there were agents who were not happy about the policy. The Director feels very strongly that it is an appropriate policy, that it does move good supervisors up in management so that they have a greater span of control, so that we can further benefit from the skill sets that they have from their tenure at the Bureau.

Mr. GOHMERT. So the answer is, no, you are not revisiting the policy? Is that your answer?

Ms. CAPRONI. That is correct.

Mr. GOHMERT. Okay. I just wanted to weed through and get to the answer. Thank you.

Now, with regard to these letters, it is deeply troubling because we have been hearing about how important they were in order to get this information. But you know—I mean, we had assurances from everybody from the AG on down that there was adequate oversight, that there was adequate training.

What suggestions—since you are not changing any personnel policies, what actual structural policies within the FBI are going to change to make sure that there would be adequate oversight just in case the NSLs were allowed in the future?

Ms. CAPRONI. Again, we are going to do substantially more training. Agents are now being placed into career paths, and they are going to be required, after their time at Quantico, to return to Quantico for sort of a postgraduate period. That will have extensive training for those agents who are on the national security career track.

We are also implementing an auditing practice that will include Department of Justice lawyers, inspectors from the FBI, and FBI lawyers to go out and methodically audit the use of the National Security Letters.

More generally, we are going to create a compliance program within the Bureau that will be interdisciplinary, and it will make sure that—not just with National Security Letters. I mean, this is one tool, and it is a tool that, as indicated in this report, we need better controls on. Our concern is that there may be other things that we need to make sure that we have gotten better controls on, that we think we have given perfectly clear guidance on, but in terms of execution in the field, we have got some problems.

So, again, I cannot say enough that we take this report extremely seriously. We know we have got issues. We know we have got problems. The Director and upper management are absolutely committed that we are going to fix this.

Mr. CONYERS. Your time has expired.

Mr. GOHMERT. Thank you, Mr. Chairman.

Mr. CONYERS. Mr. Artur Davis from Alabama is recognized.

Mr. DAVIS. Thank you, Mr. Chairman.

Ms. Caproni, give me your best legal assessment. Would the exclusionary rule apply to any evidence obtained from the improper issuance of these letters?

Ms. CAPRONI. Probably not, but I have not, quite frankly, given that a great deal of thought. It is not a fourth amendment violation. The exclusionary rule clicks in when you have got a fourth amendment violation. These records are being held by third-party businesses, so it is not a fourth amendment problem.

Mr. DAVIS. Well, would there not be fourth amendment implications if information were obtained as a result of the improper use of Federal statutory authority?

Ms. CAPRONI. There would be other problems, but I do not think there is a fourth amendment problem.

Mr. DAVIS. Well, do you think that there would be a practical problem?

A classic hypothetical: If a National Security Letter were improperly issued, and it turned out later on there was perhaps a valid basis for the issuance of a warrant, wouldn't that possibly be compromised or wouldn't the emergence of a valid basis later on be compromised by the misuse of an NSL?

Ms. CAPRONI. Again, I am always leery of responding to hypotheticals. All I can say is, there is no—we are not minimizing this. We do not want any improper use——

Mr. DAVIS. So you are not sure. Let me follow up on Mr. Schiff's questions.

Are you familiar with the name Bassem Youssef?

Ms. CAPRONI. Yes, sir, I am.

Mr. DAVIS. Mr. Youssef, as I understand it, was in charge of the Communications Analysis Unit at the Bureau; isn't that right?

Ms. CAPRONI. He was, beginning in the spring of 2005.

Mr. Davis. Is it accurate that Mr. Youssef raised concerns about the misuse of the NSLs to his superiors?

Ms. CAPRONI. That will have to be determined through the inspection. I do not know the answer to that question.

Mr. DAVIS. Well, you know that that has been reported, and I assume, Mr. Fine, neither you nor Ms. Caproni has any basis to dispute what Mr. Youssef's lawyers are saying about his making that report.

Ms. CAPRONI. I would note that Mr. Youssef is in litigation with the FBI.

Mr. DAVIS. That is not what I asked you. I asked you if you had any basis to dispute this report.

Ms. CAPRONI. I do not know one way or the other.

Mr. DAVIS. Mr. Fine, do you have a basis to dispute that there were complaints raised by the former head of the Communications Analysis Unit?

Mr. FINE. We did not review what he did, what he——

Mr. DAVIS. Mr. Fine, how is it possible that you did not review the fact that the former head of the unit raised questions about the misuse of the NSLs? How is it remotely possible that was not reviewed?

Mr. FINE. We reviewed what happened in that unit and what was issued; and we did review the discussions that occurred between the Office of General Counsel, and that included——

Mr. DAVIS. Mr. Fine, the head of the unit—not a secretary, not an intern, not a line officer—but the head of the unit raised concerns. How is it possible that you did not conduct an interview of Mr. Youssef?

Mr. FINE. We did interview Mr. Youssef, and we did not hear that concern from him. And, in fact, from the interview of Mr. Youssef and also from the review of the records, we saw that he had signed a letter. And many letters were signed——

Mr. DAVIS. Are you disputing that Mr. Youssef complained about the improper issuance of NSLs?

Mr. FINE. To his superiors?

Mr. DAVIS. Yes.

Mr. FINE. I do not know that. I do know——

Mr. DAVIS. Did you ask him?

Mr. FINE. I do not believe we—I am not sure whether we asked that question, but——

Mr. DAVIS. Mr. Fine, how do you possibly not ask the head of the unit if he had any concerns about whether or not the statute was followed? How does that possibly not come up as a question?

Mr. FINE. We did ask him, and we questioned him extensively, our attorneys did, about the communications between the Office of General Counsel, which was that——

Mr. DAVIS. Well, did he say that he raised questions?

Mr. FINE. Not that I am told, no.

Mr. DAVIS. Not that you remember or not that you were told? Which one?

Mr. FINE. Well, I actually did not do the interview, but let me just check.

[Brief pause.]

Mr. DAVIS. While you are working on the answer to that, Mr. Fine, the rather obvious observation is that I hope that your time to get the answer is not taken out of my time.

If you have the head of the Communications Analysis Unit raising questions about how that unit does its work, it is a little bit amazing to me that you are having to search your memory as to what happened during the interview.

But let me move on.

Mr. FINE. Well——

Mr. DAVIS. Is it true—well, my time is limited, Mr. Fine.

Is it true that Mr. Youssef won the Director of Central Intelligence Award in 1995 for his work infiltrating the group that tried to blow up the Trade Center in 1993?

Mr. FINE. I have heard that.

Mr. DAVIS. Do you have any reason to dispute it?

Mr. FINE. No.

Mr. DAVIS. Is it true that Mr. Youssef was the legal attache to Saudi Arabia during the time that the Khobar Towers bombing was being investigated?

Mr. FINE. I have no reason to dispute that.

Mr. DAVIS. Is it true that Mr. Youssef received outstanding personnel evaluations during that time?

Mr. FINE. I have no reason to dispute that.

Mr. DAVIS. So you have someone who was the head of a unit, who had won awards for his intelligence work, who apparently received superior evaluations, raising concerns about how his unit was being conducted; is that accurate?

Mr. FINE. I am not sure it is accurate. I am not——

Mr. DAVIS. What is inaccurate about it?

Mr. FINE. What is inaccurate is that it is not clear what concerns he raised and what he did to stop this. And we did look——

Mr. DAVIS. Again, Mr. Fine—I know my time is up. If the Chairman would indulge me for one question.

I guess I am searching for what is opaque about this. This gentleman was in a very important position; he was in charge of the unit. You admit that you interviewed him, but your memory seems foggy as to what you asked him, and your memory seems foggy as to whether or not he raised concerns to his superiors and what the concerns were.

I cannot imagine a more important interview that you could have conducted.

Mr. FINE. We did conduct that interview, and we went over extensively what the concerns were between him and the General Counsel's Office and the attempts to put the exigent letters——

Mr. DAVIS. Who did he raise these concerns with?

Mr. CONYERS. The gentleman's time has just about expired. What I would like to do is to give the Inspector General an opportunity to fully finish his answer.

Mr. FINE. We did interview Mr. Youssef, Congressman, and we did not find that, as a result of his actions, the problems were corrected. We did find, through review of the NSLs, that he signed one, that under his leadership these exigent letters continued; and we saw the efforts between the Office of General Counsel and the CAU to correct this, which did not occur, and we did not see that he put a stop to this.

However, we did not do——

Mr. DAVIS. Was he of the power to put a stop to it?

Mr. FINE. He was the head of the unit.

Mr. CONYERS. Just a moment. If my colleague will suspend, I want him to be able to complete his answer before we go on to the next Member.

Mr. FINE. We did not see that this practice was stopped during his time. There was an attempt to sort of provide NSLs reasonably soon after the exigent letters, but the exigent letters continued.

And it is important to determine who did what, when and how; and the FBI is going to do that, and we are going to look at that very carefully, as well. But our review was not to look at everybody's actions up and down the line, including his or others' to determine what steps each one of them took.

What we tried to do is present the problem and the issue and make sure that it stopped as a result of it.

Mr. CONYERS. The gentleman's time has expired.

The Chair recognizes Darrell Issa, the gentleman from California.

Mr. ISSA. Thank you, Mr. Chairman.

I guess I will start off slowly and just follow up on Mr. Gohmert for a second. It does seem amazing that an organization of excellence, as the FBI has historically been, would adopt a "We have got to get you to the Peter Principle achievement level with this up-or-out policy," and I would strongly second Mr. Gohmert, what I think he was saying, which is, if you have people who can be very good at what they do at the beat levels, so to speak, of the FBI in various positions—if they can, in fact, be superb leaders at a level that they are comfortable and, quite frankly, in a community that they are comfortable living and working in and building more capability, rapport and analysis capability and you adopt an up-or-out program—what you do is, you force them either to leave because they do not want to leave communities they are attached to or, quite frankly, you force them to a management level they may not be comfortable with.

It is bad enough that the Army will not allow a great company commander to continue being a company commander and must force them to a staff position somewhere where they endlessly see papers in the hopes that they someday will get a battalion command, but there is a certain amount of history there.

I strongly suggest that the FBI should not have a history that people doing a good job at a given level be forced on. Having said that, that is a management decision that the next Administration hopefully will straighten out.

Speaking of management decisions, General Fine, I am a little shocked that under this Attorney General, this Administration seems to look at violations of constitutional rights for limited capabilities that we have granted from this body, as the general counsel said, "troubling."

If what the FBI did was done by a private sector individual, wouldn't the FBI be arresting them? Wouldn't the U.S. attorneys be prosecuting people who played fast and loose with these rules?

Mr. FINE. It depends on the intent involved and what happened.

Mr. ISSA. Okay. Let me back up.

If there were a pattern over time, as there is, of abuses piling up to where it was clear that people knew it was happening—even some people clearly made comments that it should not be happening, that it was inconsistent with the law, but it continued—isn't that a poster child for the FBI and for the U.S. Attorney's Office to criminally prosecute people who do these things?

Mr. FINE. Again, if there were an intent to do that as opposed to a pattern of negligence, and also a knowledge of this, and we went in and looked at it after the fact and found all sorts of problems and compiled a 126-page report which lays it out in black and white, and it is, you know, a serious, serious abuse.

But at the time, were they aware of it? Did they know about that and what their intent was? That is much harder to say. We did not find evidence of criminal misconduct, but we certainly found evidence——

Mr. ISSA. Wait a second. Wait a second.

Piling up evidence that crosses the guidance we allow to pile up that evidence, and you are saying that it is not criminal?

Mr. FINE. Well, you have to look at the individual allegations as well. We looked at the files. We found in several files, in many files, that there were no abuses. We found in others that there were problems with them.

Mr. ISSA. But there are no prosecutions and no dismissals; is that correct?

Mr. FINE. Well, there are no prosecutions. The FBI is looking at the evidence right now to see what people knew and what they did not, whether it was because of any intentional conduct that they knew they were doing wrong.

We did not see that, but we did not do a review where we asked each individual, "What did you do and why?" we did a review of—an audit of this to lay out the problems for the Congress.

Mr. ISSA. Well, I would suspect that I join the Chairman and many Members on both sides of the aisle in saying, I have serious doubts about whether or not the Congress can continue to extend capabilities that are not 100 percent adhered to and there are no significant results when they are not adhered to, and then not feel that what we are doing is giving the FBI the ability to violate people's constitutional rights.

You know, I heard today, well, geez, we would not exclude this—and Congressman Schiff brought it out—we will not exclude this information even though we played fast and loose; and we will not dismiss and we will not prosecute.

Well, with all due respect, from the Attorney General on down, you should be ashamed of yourselves. We gave—we stretched what we could give in the PATRIOT Act. We stretched to try to give you the tools necessary to make America safe, and it is very, very clear that you have abused that trust, and when the reauthorization of the PATRIOT Act comes up or any bill coming down the pike, if you lose some of these tools, America may be less safe, but the Constitution will be more secure, and it will be because of your failure to deal with this in a serious fashion.

I yield back.

Mr. CONYERS. Thank you very much.

The Chair recognizes Keith Ellison, the gentleman from Minnesota.

Mr. ELLISON. Thank you, Mr. Chair.

Mr. Fine, I want to talk to you about your report recommendations starting with the exigent letters.

Wouldn't it be better simply to adopt the FBI's practice, current practice, of simply banning the use of exigent letters? I notice that

in your recommendations, or in what I believe are your recommendations, your suggestion is to take steps that the FBI not improperly use the letters, but why not just say "no exigent letters"?

Mr. FINE. Well, there should not be an exigent letter of the sort that they use. There is a process under the statute to get emergency information under certain conditions, and that is the way they ought to do it. So that is a proper use of such a request.

They surely should ban the way they did it in the past.

Mr. ELLISON. And that would be a change by statute or a rule change?

Mr. FINE. Well, it does not need to be a statute. There is a statute that allows voluntary disclosure if there is an imminent threat and danger to the safety of an individual or others, and if there is that exigent circumstance, they can get the information and use such a letter. But what they should not do is combine it with an NSL the way they did it in the past. They ought to completely separate that and follow the statute.

Mr. ELLISON. Right. So what you are saying is that the practice in which the FBI was using the exigent letters combined with the NSL was—if the statute were properly followed, then there would not be the problem that we see today; is that right?

Mr. FINE. That is correct.

Mr. ELLISON. Now, what sort of sanctions do you think should be applied, given the way that the FBI did use the NSL and the exigent letters?

Mr. FINE. I think the FBI ought to look at this and look at the individuals involved and find out if they inappropriately and knowingly misused the authorities. They ought to take appropriate action against individuals, either management individuals who allowed it to occur or individuals in the field; and if they had poor performance, that ought to be assessed as well. So I think that ought to be something that the FBI is looking at.

But I do not think they ought to say that simply because there was a misuse of the statute inadvertently that that would necessarily require misconduct charges against them.

Mr. ELLISON. Right. Well, you know, part of the problem here is that the very nature of the act that allows for the expanded use of the NSL is below the radar, and so it, by nature, lacks transparency, which is why people are so upset that the abuses took place.

But I guess my next question is, another recommendation that you have made is that there be greater control files for the NSLs. How would you envision that working?

Mr. FINE. No. There should be greater controls on the use of NSLs. They ought to make sure that the people know when they can be used and under what statute they can be used. There need to be signed copies of the NSLs so that there can be an audit trail. They have to be connected to an investigative file, not a control file.

Mr. ELLISON. Excuse me. I am sorry, Mr. Fine.

Do you see this as essentially a training problem?

Mr. FINE. I think it is a training problem. I think it is a supervision problem. I think it is an oversight problem. And I think it

is a lack of adequate internal controls and is an auditing problem as well.

Mr. ELLISON. Now, that brings me to the few questions I had for Ms. Caproni.

Ms. Caproni, do you have the staff to make all of the changes that are needed in order to have this program work properly?

Ms. CAPRONI. I would always like more resources.

Mr. ELLISON. No. I am asking you—that is not my point.

My question is, in order to—we could just simply go back to status quo, anti—back to pre-PATRIOT Act where NSLs were authorized, but not the expanded use of them that we have now. That could be one way to simply solve this problem.

But my question is, at this time, do you have the staff to provide the training, to provide the controls that are called for by the recommendations?

Ms. CAPRONI. I do. We are going to get some more staff that we have already discussed. We are going to get some analytic help, because we think that some of this would have been detected if we had had good analytic help so that we could see trends.

But I think that we have enough lawyers. I think we can do what needs to be done. We are going to have assistance from Department of Justice lawyers for some of this, but I think we have sufficient resources.

Mr. ELLISON. Ms. Caproni, if you have the sufficient resources, why didn't you use them before? I mean, I guess the question that comes up in my mind is that you either do not have the resources to effectuate the changes that have been recommended or you do. And if you do, why weren't they applied?

Ms. CAPRONI. This report told us a lot that we just did not know. I mean, I will fall on that sword again, which is that we learned a lot from this report, and we are going to make changes.

I think I have got the personnel to do it. I think we have got the resources. We are going to make the resources available.

This is important to us. It is important to us to regain the confidence of the American people and to regain the confidence of this Committee. You are one of our oversight Committees, and you are very important to us, and we are not—trust me, I am not happy that we have this report and that I am in the position of saying, you know, we failed.

Mr. ELLISON. Ms. Caproni, if I could just go back to Mr. Fine.

Mr. Fine, one of the changes that was made in the PATRIOT Act was to say that, I think, people other than headquarters officials could issue these letters.

Should the authority for the issuance of the letters be retracted to what it was before the PATRIOT Act?

Mr. FINE. I am not sure of that, and I do not want to necessarily give legislation that should occur.

I do think it is important, if that authority is out there, that it has to be overseen; and bringing things back to headquarters may or may not be the answer. As you will recall in the September 11th attacks with the Moussaoui case, one of the concerns was headquarters was controlling the field too much, and so there are considerations on both sides of this issue. I do think that when it does

go out there, it has to be used appropriately and overseen appropriately.

Mr. ELLISON. But if you had a narrower route through which these letters were authorized, wouldn't you have greater accountability?

Mr. FINE. You could. You could have greater accountability.

On the other hand, the effect of this could be diminished significantly, so I think that is the balance that has to be struck.

Mr. CONYERS. The time of the gentleman has expired, but I would like to say to Mr. Ellison that he has raised a point that we need to try to figure out at this hearing: Are there in existence the resources that are required and needed to reveal all of these people who have been abused or who have been violated by this system?

For this hearing to close down—the gentleman from California, Mr. Berman, will be recognized next—without our having figured out, for example, that we do not have anywhere near the resources, as I have been talking with the gentleman from California, Mr. Lungren, about, either in the Federal Bureau of Investigation or in the Office of the Inspector General.

If resources do not exist here, we may end up very well correcting everything from this point on, but how many thousands of people will have been violated to whom we will all be saying, from now on, not to worry, that it is all over with?

That is a troubling consideration, Mr. Lungren, that we have had under discussion, that I am still looking for the answer to.

So I recognize the gentleman from California, Mr. Berman.

Mr. BERMAN. Well, thank you very much, Mr. Chairman.

Mr. Fine, section 126a of the PATRIOT Act requires that not later than 1 year after the date of enactment of this act the Attorney General shall submit to Congress a report on any initiative of the Department of Justice that uses or is intended to develop pattern-based data-mining technology.

The 1-year deadline expired on March 9th of this year. To my knowledge, we have not received this report. Can you give us an update on the progress of this report?

Mr. FINE. From the Attorney General, no, I cannot give you progress. That is not my office. But I certainly can bring back that question to the Department.

Mr. BERMAN. But I thought——

Ms. CAPRONI. Congressman, I, unfortunately, can tell you. Yes, it was not submitted on time. I think we sent a letter indicating that it is still being worked on. I saw a draft going back across between us and the DOJ, so it is being worked on.

Mr. BERMAN. Okay. Well, then, let me ask you.

As I understand the audit that the Inspector General has undertaken, information from the National Security Letters is routinely added to the FBI's internal automated case system, which has about 34,000 authorized users; and then it is periodically downloaded into the Investigative Data Warehouse, which has approximately 12,000 users.

Is it possible that other agencies of the Federal Government, or anywhere, are using information in that Investigative Data Warehouse for data-mining purposes?

Ms. CAPRONI. For data-mining purposes, I do not know the answer to that. I mean, they could get access to it as appropriate for their agency.

Mr. BERMAN. So it is possible?

Ms. CAPRONI. I do not know the answer. I do not know.

Mr. BERMAN. You do not know if it is possible, or you do not know if they are?

Ms. CAPRONI. I do not know what they are doing with it, and I do not know what rules and restrictions govern them, so I just cannot answer that question.

Mr. BERMAN. Well, let me get one thing clear.

Is the report that we are awaiting an Inspector General's report or an Attorney General's report?

Ms. CAPRONI. An Attorney General's.

Mr. BERMAN. An Attorney General's report. All right.

So will that report include the data-mining of information in the Investigative Data Warehouse by agencies not within the Justice Department? This report that you have seen circulating, will it include the data-mining of information by other agencies from the Justice Department's Investigative Data Warehouse?

Ms. CAPRONI. It does not, but I do not know whether that means that no such activities are occurring or because it is not within the scope of the request.

Mr. BERMAN. Well, since I was involved in this language, we think that since the database is under the purview of the Department of Justice, the use of it by other agencies would be included in that report under section 126a.

Ms. CAPRONI. I will make sure that the people at DOJ understand that that is your interpretation of it.

Unfortunately, I have been in the world of NSL and this report, and I have not been in the world of the data-mining report, so I just have not read it, so that is why I cannot answer your question.

Mr. BERMAN. So you have not been personally involved in determining whether other agencies are being cooperative on how they are using the data from the—I take it you do not.

Ms. CAPRONI. I do not. I just have not been involved in it.

Mr. BERMAN. If you, subsequent to this hearing, could get that information and pass it on to me, I would be very grateful.

Ms. CAPRONI. Certainly, I can.

Mr. BERMAN. The information about whether the report will talk about other agencies' use of the Justice Department's Investigative Data Warehouse for data-mining purposes.

Ms. CAPRONI. Again, I will make sure that the Department understands your position.

Mr. BERMAN. Thank you.

Mr. LUNGREN. Would the gentleman yield to me——

Mr. BERMAN. I would be happy to.

Mr. LUNGREN [continuing]. So I could ask a question?

Ms. Caproni, one question just came to mind, and that is, part of this testimony today has talked about how agents in the field and special agents in charge in the field did not get the proper legal advice from, I presume, people who report to you, that they were not challenged as to the legal sufficiency of the NSLs or of the exigent letters; is that correct?

Ms. CAPRONI. I think that comment was relative to the lawyers in the field, who actually do not report to me.

Mr. LUNGREN. Whom do they report to?

Ms. CAPRONI. They report to the special agents in charge. They report to their field office head. That is one of the things that Mr. Fine has suggested that we look at, and that is actively under discussion at the Bureau right now, whether that reporting structure should change.

Mr. LUNGREN. So they do not report to you at all?

Ms. CAPRONI. No, sir, they do not.

Mr. LUNGREN. So they were on their own in the advice they were giving of a legal nature to the agents and to the special agents in charge to whom they report?

Ms. CAPRONI. On a reporting basis, they do not report to me. I do not supervise them.

I am in charge of the legal program. So we provide the CDCs. That is their title. We provide them with substantial legal advice, and they frequently call us when they have questions, but I do not rate them, and they do not report to me. I do not hire them; I do not fire them.

Mr. LUNGREN. I know, but what I am trying to figure out is, if these attorneys report to the SAC, does that make it more difficult for them to tell the SAC that he or she is wrong when they are asking for one of these letters?

Ms. CAPRONI. That is the concern that Mr. Fine has raised. I mean, I——

Mr. LUNGREN. Well, do you share that concern?

Ms. CAPRONI. I do share that concern.

Mr. LUNGREN. Could that be one of the real problems we have got here?

Ms. CAPRONI. I will say there are arguments both ways, Congressman. It is not—and the reason I say that is because I report to the Director of the FBI, and I do not have any problem telling the Director of the FBI my legal advice; and if he does not like it, it is still my legal advice.

That is what the CDC should be doing, but whether they——

Mr. LUNGREN. My experience has been that the SACs are pretty important people in their various offices, and most people generally think they are the top dogs, and we have this problem where, apparently, good legal advice either was not given or was not accepted, and maybe that is something we ought to look at if you folks will not look at it.

Ms. CAPRONI. Again, we are actively looking at that very question of whether the CDC reporting structure should change.

Mr. LUNGREN. And I thank the gentleman from California for yielding, although he is not here to receive it back.

Mr. CONYERS. I thank you all.

The gentleman from Minnesota had one last question that I have agreed to entertain, if you will.

Mr. ELLISON. Thank you, Mr. Chair.

My question is, of all of the letters that have been issued and of all of the inaccurate and improper data that has been set forth, clearly some information came back; and in the cases where indi-

viduals' information was obtained in violation of the rules and of the statutes, what has happened?

Have these individuals been notified? What recourse do they have? What is the story on the people?

Ms. CAPRONI. The people are not notified. Their records are removed from our databases, and the records are destroyed.

Mr. FINE. That is correct.

Mr. CONYERS. Thank you very much.

Ladies and gentlemen, this has been an excellent hearing. We thank the witnesses for continuing in an extended period of examination. We will all be working together. There are 5 legislative days in which Members may submit additional questions to you and send them back as soon as you can.

We also want to enter into the record Caroline Fredrickson's statement on behalf of the American Civil Liberties Union, Congressman Coble's Department of Justice facts sheet release. We also have *The New York Times,* which officially alerted the FBI to rules abuse 2 years ago, dated March 18th. And we also have a letter being hand-delivered to the general counsel, dated today, March 20th, which asks her for additional information.

The record will be open for 5 additional days, and without any further business before the Committee, the hearing is adjourned. We thank you for your attendance.

[Whereupon, at 12:45 p.m., the Committee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND MEMBER, COMMITTEE ON THE JUDICIARY

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2435 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
CRIME, TERRORISM, AND HOMELAND SECURITY
RANKING MEMBER
IMMIGRATION, BORDER SECURITY, AND CLAIMS
HOMELAND SECURITY
SUBCOMMITTEES:
INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESMENT
ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY
MANAGEMENT, INTERGRATION, AND OVERSIGHT
SCIENCE
SUBCOMMITTEES:
ENERGY
SPACE AND AERONAUTICS
MEMBER:
DEMOCRATIC CAUCUS POLICY AND STEERING COMMITTEE
CO-CHAIR:
CONGRESSIONAL CHILDREN'S CAUCUS

CONGRESSWOMAN SHEILA JACKSON LEE, OF TEXAS

STATEMENT BEFORE THE

JUDICIARY COMMITTEE

HEARING ON "INSPECTOR GENERAL'S INDEPENDENT REPORT ON THE F.B.I.'S USE OF NATIONAL SECURITY LETTERS"

MARCH 7, 2007

Thank you, Mr. Chairman for holding this hearing. Let me also welcome and thank our witnesses, Mr. Glenn A. Fine, the Inspector General for the U.S. Department of Justice; and Ms. Valerie Caproni, the General Counsel of the Federal Bureau of Investigation.

The purpose of today's hearing is to review the Inspector General's Report on the FBI's Use of National Security Letters

(NSLs). That report has raised widespread concerns regarding the manner in which federal agencies investigate individuals. The Inspector General's Report identified several serious issues regarding the FBI's methods of reporting to Congress its use of NSLs, the manner in which it collects, retains, and uses information, and the implications these methods have on individual privacy rights.

Specifically, the Report states that that the FBI has reported inaccurate and incomplete data to Congress. Additionally, the report documents improper methods used by the FBI to acquire data on individuals. Exacerbating matters, it appears that the FBI has retained information collected on individuals indefinitely even in cases where the individual involved has no direct or substantial relevance to any terrorism investigation. This pattern of conduct, of course, raises serious concerns regarding the privacy rights and civil liberties of American citizens and residents.

Mr. Chairman, "National Security Letters" (NSLs) are written directives to provide information that the FBI issues directly to third parties, such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies. Under current law, NSLs are not subject to judicial review. Over the last 20 years,

Congress has enacted a series of laws authorizing the FBI to use NSLs to obtain four types of information in terrorism, espionage, and classified information leak investigations without obtaining warrants from the Foreign Intelligence Surveillance Court or approval from another court. The four types of information are:

1. financial institution customer records;
2. certain communication service provider records;
3. certain financial information and consumer reports, and credit agency consumer records for counterterrorism investigations; and
4. financial information, records, and consumer reports.

Prior to September 11, 2001, and the enactment of the Patriot Act, the authorizing statutes which governed NSLs required that prior to their issuance a senior FBI Headquarters official certify that the FBI had "specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or agent of a foreign power" as defined in the Foreign Intelligence Surveillance Act of 1978.

In the wake of the September 11, 2001 attacks, the Administration expressed concern about the delays in effectuating the preparation and ultimate dissemination of NSLs and prevailed upon the Congress to enact the USA PATRIOT Act, which, *inter alia*, relaxed the standard that must be satisfied to warrant the issuance of

a national security letter. The Patriot Act substantially expanded the FBI's preexisting authority to obtain information through NSLs in four ways. First, it eliminated the requirement that the information sought in an NSL must pertain to a foreign power or an agent of a foreign power and replaced it with the lesser showing that the information requested was "relevant to or sought for an authorized investigation to protect against international terrorism or espionage. Second, it authorized the issuance of NSLs by heads of FBI field offices and instead of senior FBI headquarters officials.

Third, it permitted NSLs to request information from communications providers, financial institutions, and consumer credit agencies about persons other than the subjects of FBI national security investigations so long as the requested information is relevant to an authorized investigation. Finally, it allowed any federal government agency (not merely the FBI) investigating or analyzing international terrorism to obtain a consumer's full credit report.

When it reauthorized the PATRIOT Act in 2005, Congress directed the Department of Justice's (DOJ) 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." The OIG was also directed to review the use of NSLs for two time periods: calendar years 2003 through 2004, and calendar years 2005 through 2006. The first report was turned into Congress this month. The second report is due on December 31, 2007.

Congress directed the OIG's review to include the following:

1) An examination of the use of NSLs by the DOJ 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;

3) an examination of the effectiveness of NSLs as an investigative tool, including-

A) the importance of the information acquired by the DOJ to the Intelligence activities of the DOJ 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 DOJ, including any direct access to such information (such as 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 DOJ utilized such information to produce an analytical intelligence product for distribution within the DOJ, to the intelligence community . . . or to Federal, State, local, or tribal government departments, agencies or instrumentalities;

> D) whether, and how often, the DOJ provided such information to law enforcement authorities for use in criminal proceedings; . . . .

Further piquing Congress's interest in the FBI's use of NSLs was a November 6, 2005 Washington Post article that reported that the FBI issued 30,000 NSLs every year, a hundred fold increase over historical practices. The article suggested that the FBI was using NSLs to spy on ordinary Americans. In effect, the article highlighted the breadth of the use of NSLs.

The Report completed and submitted by the OIG documents at least six different types of troubling findings. First, the FBI's practice of collection and retention of information obtained from NSLs was problematic because the FBI had no policy or directive requiring the retention of signed copies of NSLs or any requirement to upload NSLs in the FBI's case management system. Second, in many important respects the data rRegarding National Security Letters issued by the FBI from 2003 through 2005 was incomplete and inaccurate.

Third, the volume of National Security Letter requests involving persons in the United States increased dramatically during the period 2003 through 2005. Fourth, notwithstanding the FBI's claims that NSLs are an effective investigative tool, the FBI did not possess data

to substantiate the efficacy of NSLs' in criminal investigations and prosecutions. Fifth, the OIG Report identified many instances where NSL were used improperly or illegally. Last, the OIG Report documents numerous instances where the FBI failed to comply with its own policies and guidelines regarding the issuance and use of NSLs.

The purpose of this hearing to learn more about what went wrong with the NSL process and what, if anything, can be done to fix it. I am pleased that we have before us today the author of the OIG Report and the chief legal officer of the FBI to shed light on this important subject. I look forward to their testimony.

Thank you, Mr. Chairman. I yield back my time.

PREPARED STATEMENT OF THE HONORABLE LINDA T. SÁNCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA, AND MEMBER, COMMITTEE ON THE JUDICIARY

Congresswoman Linda T. Sánchez

Statement for The Record
March 20, 2007
Full Committee Hearing on "The Inspector General's Independent Report on the F.B.I.'s Use of National Security Letters."

We all agree that protecting our nation and fighting terrorists is a national priority. But our democracy is not so cheap that we should advance our security at the expense of our civil liberties.

In 2004, the District Court for the Southern District of New York, concluded that the practice of issuing National Security Letters violates the Fourth and First Amendments. The court stated that they have "the effect of authorizing coercive searches effectively immune from any judicial process."

We face very real threats from terrorists who have no respect for life, liberty, or democracy, but we cannot jeopardize the great principles this country was founded on. If we continue to allow the Constitution to be chipped away we will have let those that hate this country win. If we protect our nation by destroying our deepest principles, we need no outside enemies. We will have done the job for them.

I applaud the Inspector General, Mr. Fine, for shedding some light on the misreporting of National Security Letter issuances. But I am still concerned that the system charges the Executive Branch with policing itself. And as this report demonstrates, that system is not working.

At the very best, this report reveals sloppy reporting; at the very worst, it is evidence of a deliberate attempt to hide the truth from Congress and the American people.

Over the past few weeks this Committee has learned information about the Department of Justice that – even when taken individually – is very disturbing. When one looks at the big picture a pattern of abuse and cover-up emerges.

I do not advocate for practices that would hinder terrorism investigations, and ultimately put American citizens in jeopardy. But I believe that we have enough other tools to robustly protect our country without jeopardizing the rights and liberties of our citizens –the rights that make our nation worth protecting.

It is my hope that this hearing is just the start of this Committee's oversight activities on this matter. I thank the Chairman for his leadership in holding this very important hearing.

Thank you, Mr. Chairman.

RESPONSE TO POST-HEARING QUESTIONS FROM GLENN A. FINE, INSPECTOR GENERAL, U.S. DEPARTMENT OF JUSTICE

Response to April 19, 2007, Questions From Chairman Conyers' Follow-up to March 20, 2007, Hearing Before the House Judiciary Committee

1. Your report mentions some problems reconstructing the actual number of NSL requests. Will we ever know how many requests were actually made or even whether they all were grounded in an "authorized" investigation?

ANSWER: The FBI has stated that it is attempting to correct the data previously reported to Congress on national security letter (NSL) usage by correcting its database and, through a random sampling of 10 percent of the total entries in the database, manually checking the entries against relevant entries in its Automated Case Support System (ACS). Based on the results of this audit, the FBI has stated that it will supplement some of its prior reports to Congress. However, these steps will only provide estimates of the total number of NSLs issued during the relevant time periods. Moreover, we cannot say at this point whether these efforts will enable the FBI to document that each NSL was grounded in an authorized national security investigation.

For future reporting, the FBI has stated that it is developing a "workflow tool" that it believes will automate much of the work that is associated with preparing NSLs and related paperwork. The OIG will be closely monitoring these developments and will report its findings and analysis in our report due to Congress at the end of this year.

2. On page 109 of your Report, you explain that FBI agents are accessing "NSL information about parties two or three steps removed from their subjects without determining if these contacts reveal suspicious connections."

- Does this activity violate the standard that information sought must be relevant to an authorized investigation?

ANSWER: The NSL statutes do not require the FBI to examine the results of initial NSLs relating to the investigative subject before issuing NSLs on persons two or three steps removed from the subject. So long as the authorizing official certifies that the information requested is "relevant" to, sought for, or necessary for an authorized investigation (depending on the NSL statute involved), the FBI may request information two or three steps removed from a subject at the outset of its investigations. In our recent review, we did not see the FBI routinely asking for NSL information two or three steps removed from its investigative subjects, but we identified some instances where this

occurred. We also noted periodic concerns about this issue in communications between attorneys in the FBI's Office of the General Counsel's National Security Law Branch (NSLB) and various field-based Chief Division Counsels. The absence of any guidance on the use and sequencing of national security letters also raised concerns that their use could, in some cases, be inconsistent with the proviso in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) requiring that the FBI use the "least intrusive collection techniques feasible" in its investigations. For this reason, we recommended that the FBI provide guidance and training on the application of the Attorney General Guidelines' proviso on using the "least intrusive collection techniques feasible" to the use and sequencing of national security letters.

3. Besides the FBI's relationship with the three telephone companies, did you find other instances in which the FBI formed close private sector relationships?

- How do these private sector relationships affect the integrity, if at all, of the FBI's operations?

ANSWER: The only private sector relationships that related to our review of the FBI's use of national security letters concerned the FBI's contractual relationship with the three telephone companies. We found that the expectations of the FBI's Communication Analysis Unit and the telephone companies, as reflected in contracts and other documents we reviewed, appeared to contemplate compliance with NSL statutes, Attorney General Guidelines, and internal FBI policy. However, we found that the use of exigent letters to obtain information from these three telephone companies did not comply with these requirements.

4. How would you equate the FBI's practice of using Certificate Letters with the Federal Reserve Bank with its use of exigent letters with the three telephone companies?

ANSWER: As noted in our report, we believe the FBI circumvented the Electronic Communication Privacy Act when it issued exigent letters to obtain records from the three telephone companies. We also believe the FBI violated the NSI Guidelines and its internal policies in issuing the exigent letters. In contrast, when we analyzed the FBI's practice of obtaining certain records known as Fedwire data from the Federal Reserve Bank of New York in response to certificate letters rather than Right to Financial Privacy Act (RFPA) national security letters, we could not reach a definitive conclusion as to whether the practice violated the RFPA. The reason we could not reach a definitive conclusion was that it is unclear whether Federal Reserve Banks are "financial institutions" for

purposes of the RFPA statute and whether Fedwire records are "financial records" under the statute.

With respect to the FBI's use of both the exigent letters and certificate letters, we noted in our report concerns about the ability of NSLB attorneys to obtain accurate, timely, and complete information from personnel in the Counterterrorism Division and the fact that NSLB attorneys were not consulted prior to the institution of these practices.

5. On April 6, 2006, the U.S. Attorney General responded to a question that was posed for the record by members of this Committee relating to the status and efficiency of the automated tracking system that would electronically connect the field divisions, FBI Headquarters, the FBI's National Security Law Unit, and the Office of Intelligence Policy Review (OIPR). The Attorney General responded that the Foreign Intelligence Surveillance Act Management System (FISAMS) has continued and has been highly efficient -- now with over 5,000 registered users. Based on your report, is it likely that the FISAMS, to the contrary, has not been functioning at all?

ANSWER: We did not review FISAMS as part of our national security letters or Section 215 reviews, and we therefore are not able to answer this question.

6. The Attorney General indicated that the Assistant Director of the FBI's National Security Branch issued a communication, dated January 24, 2006, reiterating the importance of accuracy in the FISA process, followed by a directive, dated February 2, 2006, requiring case agents to open and maintain FISA-subfiles containing written substantiation for each factual assertion contained in the FISA declaration. Please provide copies of this information to the Committee since issuance of the February 2 directive.

ANSWER: We did not review these directives in connection with our national security letters or Section 215 reviews. Consistent with our normal practices with regard to requests for FBI documents, we refer the Committee to the FBI to obtain copies of these documents.

7. On February 6, 2006, the FBI instituted a FISA Renewal Review Board, consisting of managers from OIPR, FBI, and the Criminal Division's Counterterrorism and Counterespionage Sections, to evaluate FISA renewal requests at regular intervals and to terminate non-productive FISAs, facilitating the more efficient use of limited resources. Can you comment on the substance and frequency of this Board's evaluation? Are the evaluations issued in writing? What is the ratio of "productive" FISA renewal requests and "non-productive" ones?

ANSWER: This subject was beyond the scope of the OIG's report on the FBI's use of national security letters. We believe the Committee should address this question, in the first instance, to the FBI and the Department's National Security Division.

8. The Attorney General has told the Committee about the advent of a half billion dollar "Sentinel" case management system for DOJ investigative matters. He alluded to its proposed expansion to include the work of U.S. Attorneys. Has this expansion occurred, and if so, what divisions of the Department are interoperable with the U.S. Attorneys?

ANSWER: This question discusses two separate systems being developed within the Department of Justice: Sentinel and the Litigation Case Management System (LCMS). Below is a brief summary of each project followed by our understanding of the interoperability of the systems.

The Sentinel case management system, initiated in 2005, is an ongoing FBI project to provide the FBI with an electronic case system, moving the FBI away from its current paper-based case management system. The Sentinel upgrade, if implemented successfully, should allow for significant improvements and efficiencies within the FBI, including the immediate dissemination of case file information within the FBI. According to the FBI, the project is scheduled to be completed in December 2009. Sentinel, which is being developed and implemented in four phases, is currently nearing the completion of its first phase. While the project is being developed by the FBI, the case management system is being built to utilize a framework of applications that may be able to be used by other investigative agencies within and outside the Department of Justice once the system is fully operational. The OIG is currently completing the third in a series of audits on the development and implementation of Sentinel.

Separate from Sentinel, the Department of Justice awarded a contract to Computer Sciences Corporation in May 2006 for the development of the LCMS. This project is scheduled to be completed in 2010. The LCMS is intended to provide the Department's litigating divisions greater data sharing capabilities through a centralized database with unique interfaces for the various divisions. The implementation of the LCMS is also to be phased, starting with the U.S. Attorney's Offices followed by other litigating divisions.

Based on our preliminary audit work on Sentinel, we believe that Sentinel and the LCMS may be interoperable on some level once both projects have been implemented. Sentinel is being built using the National Information Exchange Model (NIEM), a set of enterprise-wide

information exchange standards and processes. Although we have not audited the LCMS project and have limited information about it, we believe that the LCMS will likely also be implemented using the NIEM standards. This data exchange capability could allow the FBI to provide case information directly to the litigation divisions as cases move from investigation to litigation.

POST-HEARING QUESTIONS POSED TO VALERIE CAPRONI, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION, FROM CHAIRMAN JOHN CONYERS, JR.[1]

JOHN CONYERS, JR., MICHIGAN
CHAIRMAN

LAMAR S. SMITH, TEXAS
RANKING MINORITY MEMBER

U.S. House of Representatives
Committee on the Judiciary
Washington, DC 20515–6216
One Hundred Tenth Congress

April 19, 2007

Ms. Valerie Caproni
Office of General Counsel
Federal Bureau of Investigation
950 Pennsylvania Avenue, NW
Washington, D.C. 20530-0001

Dear Ms. Caproni:

Thank you for your recent appearance before the House Committee on the Judiciary. Your testimony on the Federal Bureau of Investigation's use of National Security Letters was insightful and will assist the Committee in its consideration of this issue.

Enclosed you will find additional questions from members of the Committee to supplement the information already provided at the March 20, 2007, hearing. The Committee is also still awaiting your responses to the questions contained in the March 20th letter that was delivered to you at the hearing.

Also, please find a **verbatim** transcript of the hearing enclosed for your review. The Committee's Rule III (e) pertaining to the printing of transcripts is as follows:

> *The transcripts...shall be published in **verbatim form**, with the material requested for the record...as appropriate. Any requests to correct any errors, other than transcription, shall be appended to the record, and the appropriate place where the change is requested will be footnoted.*

Please deliver your transcript edits and written responses to the Committee on the Judiciary by May 4, 2007. Please send them to the Committee on the Judiciary, Attention: Renata Strause, 2138 Rayburn House Office Building, Washington, DC, 20515. If you have any further questions or concerns, please contact Renata Strause at (202) 225-3951.

Sincerely,

John Conyers, Jr.
Chairman

cc: Lamar S. Smith

Enc

[1] At the time of publication, responses to post-hearing questions posed to Valerie Caproni had not been received by the Committee on the Judiciary.

Ms. Valerie Caproni
Page Two
April 19, 2007

1. Where exactly does the information obtained through NSLs reside and how is it shared with other agencies? For example, does the information feed into the DOJ Regional Sharing Systems or the DHS Automated Targeting System? Which government databases does it feed into? If you do not have an accurate sense of how the data is shared or in how many systems it currently resides, how will the Bureau go about developing a purging policy for irrelevant data or data gathered on innocent persons?

2. The I.G.'s report indicated that the FBI does not keep adequate track of the number of U.S. persons affected in their data collection. How can we accept assurances about civil liberties without accurate information regarding how many American residents have had their personal, financial or internet records in the FBI's database?

3. How much tax-payer money were the three telephone companies (AT&T, Verizon, and an unknown company) paid for their contracts with the FBI to release telephone records? What specific statutory authority was the basis for the three contracts? Please provide the Committee with copies of these contracts as well as the three memos requesting approval of the contracts, and all related executive correspondence?

4. There is a claim that the FBI's General Counsel's office was initially unaware of the existence of these contracts, but aren't the procurement attorneys who approved the contracts part of the General Counsel's office?

   -What is the general procedure for approval of such contracts?

   -How can we be assured that the General Counsel's office will not be out of the approval process in the future?

5. Were you aware at the time of the 9 NSLs in one investigation that requested subscriber information on 11,100 separate telephone numbers in 2004? When did you first learn of that volume of requests?

6. According to a March 20, 2007 Washington Post article, the FBI has told its agents that they may still ask phone companies to voluntarily hand over toll records in emergencies by using a new set of procedures. The article further stated that agents may request the records verbally in the most dire emergencies, without providing NSLs or subpoenas. This suggests that the policy of addressing the exigent letters is to simply require that no documentation is necessary. How does that solve the inherent problems surrounding the use of the exigent letters?

Ms. Valerie Caproni
Page Three
April 19, 2007

7. In the New York Times on March 19, 2007, it was reported that Bassem Youssef, who was in charge of the Bureau's Communications Analysis Unit, discovered the egregious failure to meet the legal requirements for implementing the USA PATRIOT Act and raised concerns with superiors soon after he was assigned to the unit in early 2005.

   Specifically, his attorney cited him as recounting that "the bureau had frequently failed to document an urgent national security need — proving 'exigent circumstances,' — when obtaining personal information without a court order through the use of 'national security letters'" and that "his superiors had initially minimized the scope of the problem and the likely violation of laws intended to protect privacy."

   I understand further from the New York Times on March 19, 2007, that Mr. Youssef, who was born in Egypt, is suing the bureau for discrimination, charging that senior officials improperly suspected his loyalties in part because of his Egyptian origins. What is Mr. Youssef's current employment status with the Bureau? If he no longer is employed with the FBI, was he terminated and on what basis?

8. The Attorney General indicated that the Assistant Director of the FBI's National Security Branch issued a communication, dated January 24, 2006, reiterating the importance of accuracy in the FISA process, followed by a directive, dated February 2, 2006, requiring case agents to open and maintain FISA-subfiles containing written substantiation for each factual assertion contained in the FISA declaration. Please provide copies of this information to the Committee since issuance of the February 2 directive.

9. On February 6, 2006, the FBI instituted a FISA Renewal Review Board, consisting of managers from OIPR, FBI, and the Criminal Division's Counterterrorism and Counterespionage Sections, to evaluate FISA renewal requests at regular intervals and to terminate non-productive FISAs, facilitating the more efficient use of limited resources. Can you comment on the substance and frequency of this Board's evaluation? Are the evaluations issued in writing? What is the ratio of "productive" FISA renewal requests and "non-productive" ones?

10. The Attorney General has told the Committee about the advent of a half billion dollar "Sentinel" case management system for DOJ investigative matters. He alluded to its proposed expansion to include the work of US Attorneys. Has this expansion occurred, and if so, what divisions of the Department are interoperable with the US Attorneys?

LETTER FROM RICHARD C. POWERS, ASSISTANT DIRECTOR, OFFICE OF CONGRESSIONAL AFFAIRS, FEDERAL BUREAU OF INVESTIGATION

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

June 14, 2007

Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

By letter to FBI General Counsel Caproni dated March 20, 2007, the Committee requested responses to questions based on the hearing held on that date concerning the FBI's use of National Security Letters. Thereafter, by letter to General Counsel Caproni dated April 19, 2007, the Committee requested responses to additional question based on this hearing.

Today we delivered our responses to both sets of questions to the Department of Justice (DOJ) for review and approval. DOJ will forward the responses to you directly following their review.

Thank you for your patience as the FBI works with DOJ to develop appropriate and thoughtful responses to these important inquiries.

Sincerely,

Richard C. Powers

Richard C. Powers
Assistant Director
Office of Congressional Affairs

Honorable Lamar S. Smith
Ranking Member
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

PREPARED STATEMENT OF CAROLINE FREDERICKSON, DIRECTOR, WASHINGTON LEGISLATIVE OFFICE, AMERICAN CIVIL LIBERTIES UNION (ACLU)

On behalf of the American Civil Liberties Union, its more than half a million members and activists, and 53 affiliates nationwide, I thank Chairman Conyers and ranking member Smith for holding today's hearing on FBI abuse of National Security Letters.

Over five years ago, in the wake of the terrorist attacks of September 11, 2001 Congress passed the USA Patriot Act,[1] giving the FBI extraordinarily broad powers to secretly pry into the lives of ordinary Americans in the quest to capture foreign terrorists. One of the changes the Patriot Act made was to expand the circumstances in which National Security Letters (NSLs) could be issued so that the information sought with such letters would no longer have to pertain to an agent of a foreign power, and would no longer be limited to the subjects of FBI investigations.[2] An NSL is a letter that can be issued by Special Agents in Charge (SAC) of the FBI's 56 field offices—without any judicial review—to seek records such as telephone and e-mail information,[3] financial information, and consumer credit information.

The four NSL authorizing statutes include the Electronic Communications Privacy Act,[4] the Right to Financial Privacy Act,[5] the Fair Credit Reporting Act,[6] and the National Security Act of 1947.[7] Subsequent legislation expanded the types of institutions from which records could be sought using NSLs. The Intelligence Authorization Act for Fiscal Year 1996,[8] amended the FCRA to give the FBI authority to obtain credit header information with NSLs, and a provision of the Patriot Act, expanded this power to allow the FBI and other government agencies that investigate terrorism to obtain full credit reports.[9] The Patriot Act also reduced the standard necessary to obtain information with NSLs, requiring only that an SAC certify that the records sought are "relevant" to an authorized counterterrorism or counter-intelligence investigation.

The ACLU opposed these unwarranted expansions of NSL power, and opposed making provisions of that statute permanent with the Patriot Reauthorization Act of 2005,[10] fearing these unnecessary and unchecked powers could be too easily abused. When Congress reauthorized the Patriot Act, it directed the Department of Justice Inspector General (IG) to review the effectiveness and use of these expanded authorities and one of the first of these reports, a review of the FBI's use of NSLs, was released on March 9, 2007.[11]

The IG's audit confirms our worst fears: that the FBI uses its NSL authorities to systematically collect private information about people who are not reasonably suspected of being involved in terrorism, and it retains this information indefinitely. The FBI ignored the scant requirements of the law and developed shortcuts to illegally gather information the FBI wanted from telecommunications companies and financial institutions. It did this without opening the investigations for which, by law, this information must be sought or be relevant to, and often without ever bothering to secure the NSLs or grand jury subpoenas it told these telecoms and financial institutions it would secure to support its claim of access to sensitive customer information.[12] This should be of great concern to all Americans, because the IG found the FBI is increasingly using this power against U.S. persons.[13] And despite the issuance of more than 140,000 NSL requests, the IG report documents only one

---

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. Law No 107–56, 115 Stat. 272 (2001)[Hereinafter Patriot Act].

[2] Id., section 505.

[3] Telephone and e-mail information that can be obtained with NSLs includes historical information on calls made to and from a particular number, billing records, electronic communication transactional records and billing records (including method of payment), and subscriber information.

[4] 18 U.S.C. section 2709 (1988).

[5] 12 U.S.C. section 3401 (2000).

[6] 15 U.S.C. section 1681 et seq. (1996).

[7] 50 U.S.C. section 436(a)(1)(2000).

[8] Pub. Law No. 104–93, section 601(a), 109 Stat. 961, codified at 15 U.S.C. section 1681u (Supp.V. 1999).

[9] Patriot Act section 358(g)(2001).

[10] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. Law No. 109–177, 120 Stat. 192 (2006).

[11] Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters, March 2007, http://www.usdoj.gov/oig/reports/FBI/index.htm (Hereinafter IG Report).

[12] IG Report at 94.

[13] IG Report at 38.

terrorism conviction—for providing "material support" for terrorism—and only 153 "criminal proceedings" resulting from the extensive use of this power.[14] "Criminal proceedings" is defined as all federal grand jury proceedings, as well as search warrants, indictments and trials.[15]

For over five years the Federal Bureau of Investigation has collected vast troves of data in secret and without accountability. I hope this hearing is only one of many to reestablish checks and balances on the executive branch and curb its many abuses of power. The ACLU asks this committee to hold the FBI and this administration accountable for these abuses and to make statutory changes that will ensure that they cannot happen again.

THE INSPECTOR GENERAL'S FINDINGS

Despite statements to the contrary, the Inspector General found much more than just sloppy management and poor record keeping. The Inspector General's report documents systematic failures to meet statutory requirements, and at times, intentional refusals to comply with the law.

Intentional Violation of the NSL Statute

Most disturbingly, the Inspector General's report shows that the FBI's Communications Analysis Unit (CAU) declared itself unconstrained by the NSL statutes—arguing that the law was "insufficient" for CAU's purposes—and it contracted directly with three telephone companies to access information illegally.[16] The information included telephone toll and call detail records and the contract specified that the telephone companies would provide "near real-time servicing" of these requests. The contracts were approved by the FBI's Office of General Counsel (OGC), and fulfilled by issuing so-called "exigent" letters that were used even when no exigent circumstances existed.[17] The IG was able to confirm the use of 739 exigent letters to obtain information on 3,000 telephone accounts, in the clear absence of statutory authority to do so.[18] The true number is unknown because the FBI does not keep adequate records. That FBI Office of General Counsel procurement attorneys were involved with these contracts confirms that the telecommunication companies were paid for their cooperation and silence, and confirms that contrary to the IG's assertion that the FBI's use of "exigent" letters was undertaken without the benefit of advance legal consultation,[19] FBI lawyers were instrumental in establishing this illegal process.

CAU staff, who were not authorized to sign NSLs, used "exigent" letters containing obviously false statements to obtain documents from the telephone companies when no authorizing investigation was open, when no NSLs or subpoenas had been requested, and when no emergency situation existed.[20] They then asked FBI field offices to open investigations so NSLs could be issued without telling the field office personnel that CAU staff had already received the records,[21] a clear indication that they knew what they were doing was improper. FBI National Security Law Branch (NSLB) attorneys were made aware of this issue in late 2004, possibly through complaints from field agents who resisted CAU's directives, and an NSLB Assistant General Counsel concluded that the practice of using "exigent" letters did not comply with the NSL statute. Yet, rather than prohibiting the practice outright, the NSLB attorney counseled CAU for two years regarding how and when CAU officials should use them. Regardless of this advice, CAU continued using these "exigent" letters, and the practice wasn't "banned" until the IG issued its report.[22] Even today the FBI is unable to determine whether data requested with "exigent" letters was ever covered with properly issued NSLs or subpoenas.[23]

And the issuance of "exigent" letters was only one of the illegal methods the FBI used to circumvent the NSL statutes. Using a similar scheme, the Terrorist Financing Operations Unit issued "Certificate Letters" to obtain the financial records of at least 244 named individuals in violation of the Right to Financial Privacy Act.[24]

---

[14] IG Report at 63, 64.
[15] IG Report, footnote 103, p. 62.
[16] IG Report at 88.
[17] IG Report at 92.
[18] IG Report at 90.
[19] IG Report at 97.
[20] IG Report at 92.
[21] Id.
[22] FBI letter to Inspector General Glen Fine dated March 6, 2007 included in the appendix of the IG Report.
[23] IG Report p. 91.
[24] 12 U.S.C. section 3401 (2000). *See* IG Report at 115.

Again, agents without authority to issue NSLs used these letters to circumvent the law and gain access to private financial records, and then lied about it when confronted by NSLB attorneys. When the NSLB attorneys realized they had been misled they ordered the practice halted, but it did not stop.[25] This sequence reveals what can only be described as clearly intentional misconduct.

In other instances NSLB attorneys actually signed NSLs without reference to any authorized investigation, and more than 300 NSLs were issued out of an FBI control file that was opened specifically because there was not an authorized investigation from which to issue an NSL for the data the FBI wanted.[26]

Increasing Collection of Data on U.S. persons

When Congress expanded the FBI's authority to use NSLs, it required FBI officials to certify that the information sought with these letters is relevant to an authorized investigation. By instituting this requirement, Congress clearly intended for NSLs to be a targeted investigative power, rather than a broad power that could be used to cast a wide net. But, the IG report makes clear this is not how the FBI is using its NSL authorities. In one example, nine NSLs were used to obtain records for 11,000 different telephone numbers. And, agents and analysts often didn't even review the data they received from NSLs. They simply uploaded it into computers.[27] The IG found information received from NSLs is uploaded into three separate FBI databases, where it is retained indefinitely and retrievable by tens of thousands of FBI and non-FBI personnel,[28] even if the information exonerates the subject from any involvement in terrorism.[29] Despite this extraordinary collection effort, the IG was able to document only one terrorism conviction resulting from the use of NSLs.[30] Clearly NSLs are not being used as targeted investigative tools.

The IG also expressed concern that the FBI allows agents to use NSLs to access information about individuals who are "two or three steps removed from their subjects without determining if these contacts reveal suspicious connections."[31] The fact that NSLs are being issued from control files and "exigent" letters are being used by analytic units at FBI Headquarters suggests that this tool is not being used in the manner Congress intended. Despite the FBI's claims that NSLs are directed at suspected terrorists, the Inspector General found that the proportion of NSLs issued to obtain information on Americans is increasing. In fact, the majority of NSLs the FBI issued in 2005 were used to obtain information about U.S. persons (American citizens and lawful permanent residents of the U.S.).[32]

Datamining

Neither the NSL statutes nor Department of Justice policy require the FBI to purge from its databases sensitive personal information about persons who are found to be innocent and not tied to foreign powers.[33] The Inspector General confirmed that the FBI has taken advantage of this loophole and uploads all information—admittedly innocent or not—into national databases that are indefinitely maintained. The data received from NSLs is uploaded into a "Telephone Application Database" where a link analysis is conducted, and into an Investigative Data Warehouse where it is mixed with 560 million records from 50 different government databases.[34] Tens of thousands of law enforcement and intelligence personnel have access to the information, which is not given a disposition, leaving innocent people associated with a terrorism investigation long after their information becomes irrelevant. Intelligence products developed from this data do not cite the origin,[35] so errors in the information can never be checked against the source documents. Instead, errors will be compounded when intelligence products derived from this erroneous information are distributed throughout the intelligence community and to state and local law enforcement agencies.

Erroneous Reports to Congress and the Intelligence Oversight Board

The Inspector General found that statutorily required reports to Congress excluded at least six percent of the overall number of NSLs.[36] The number of unre-

[25] IG Report at 117.
[26] IG Report at 100.
[27] IG Report at 85.
[28] IG Report at 28, 30, and 110.
[29] IG Report at 44.
[30] IG Report at 64.
[31] IG Report at 109.
[32] IG Report at 38.
[33] IG Report at 110.
[34] IG Report at 28, 30.
[35] IG Report at 54.
[36] IG Report at 34.

ported NSLs may be higher, but record keeping is so bad at the FBI, the Inspector General was unable to even confirm a final number. A review of just 77 cases from four FBI field offices found 22 percent more NSLs in case files than the FBI General Counsel knew about. More significantly, the IG found 60% of those files deficient in required paperwork, and his review doubled the number of unlawful violations that needed to be reported to the President's Intelligence Oversight Board.[37]

PROPOSED AMENDMENTS

Regrettably, the Inspector General's report only included suggestions for internal changes within the FBI's discretion, and did not include recommendations for amending the underlying statute that is the source of these abuses. It is clear that the violations the Inspector General uncovered were the natural consequence of a statute that allows government agents to access sensitive information without suspicion of wrongdoing, in the absence of court oversight, and with complete secrecy compelled by a gag order with criminal consequences. In fact, even if management and technology problems identified in the IG's report are solved, hundreds of thousands of NSLs will continue to collect information on innocent Americans because that is exactly what the statute allows.

The ACLU recommends three statutory changes that are absolutely necessary to ensure that the law protects privacy while permitting the collection of information necessary to investigate terrorism.

Limit NSLs to Suspected Terrorists and Other Agents of Foreign Powers

First, Congress must repeal the expansion of the NSL power that allows the FBI to demand information about totally innocent people who are not the targets of any investigation. The standard should return to the requirement that NSLs seek only records that pertain to terrorism suspects and other agents of foreign powers.[38] And the FBI should not be allowed to use NSLs to investigate people two or three steps removed from any criminal or terrorist activity.

Under current law, the FBI can use an NSL to obtain information that the FBI asserts is "relevant" to an investigation. The FBI has clearly taken advantage of this "relevance" standard and issued NSLs to obtain information on innocent American people with no connection to terrorism. In fact, it obtained this information without even opening an investigation to which the information must be relevant. NSLs are now issued to collect records just for the sake of building databases that can be mined later. In addition to being wholly ineffective as an investigative technique, this data collection and warehousing is an affront to the privacy of U.S. persons.

Restrict the Gag Provisions and allow for Meaningful Challenges

The gag provisions of the NSL statutes unconstitutionally inhibit individuals receiving potentially abusive NSLs from challenging them in court. Congress should amend the NSL statute so that gag orders are imposed only upon the authority of a court, and only where necessary to protect national security. Judicially imposed gag orders should be limited in scope and duration.

Further, gags must come with a meaningful right to challenge them before a neutral arbiter. Last year's amendments created a sham court proceeding, whereby a judge is powerless to modify or overturn a gag if the federal government simply certifies that national security is at risk, and may not even conduct any review for a full year after the NSL is issued. Under the NSL statute, the federal government's certification must be treated as "conclusive," rendering the ability to go before a judge meaningless. To comport with the First Amendment, a recipient must be able to go before a judge to seek meaningful redress.

Court Review

If there is one undeniable conclusion that Congress can draw from the Inspector General's report, it is that the FBI cannot be left to police itself. Allowing the FBI to keep self-certifying that it has met the statutory requirements invites further abuse and overuse of NSLs. Contemporaneous and independent oversight of the issuance of NSLs is needed to ensure that they are no longer issued at the drop of a hat to collect information about innocent U.S. persons. Court review will provide those checks and balances as was intended by the Constitution.

---

[37] IG Report at 78.

[38] Agent of a foreign power is defined in the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (1978).

CONCLUSION

The Inspector General reviewed just a tiny proportion of NSLs issued by the FBI from 2003 through 2005, yet he found an extraordinary level of mismanagement, incompetence, and willful misconduct that clearly demonstrates that the unchecked NSL authorities given to the FBI in the Patriot Act must be repealed. The FBI and Department of Justice have shown that they cannot police themselves and need independent oversight. The American Civil Liberties Union applauds the Committee for holding this hearing and opening a window on these abuses, but there is more work to be done. Congress must fully investigate the FBI's abuse of power to insure that those responsible for these violations are held accountable, and the innocent people who have had their privacy invaded and their civil rights abused need to be identified and notified, and records that have been improperly or inappropriately seized should be purged from FBI databases. But most importantly, Congress needs to fix the Patriot Act, which has set the stage for all of these problems.

LETTER REQUESTING ADDITIONAL INFORMATION SUBMITTED TO VALERIE CAPRONI, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION

JOHN CONYERS, JR., Michigan
CHAIRMAN

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

U.S. House of Representatives
Committee on the Judiciary
Washington, DC 20515–6216
One Hundred Tenth Congress

March 20, 2007

Ms. Valerie Caproni
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Ms. Caproni:

As part of our oversight regarding the Inspector General's Review of the F.B.I.'s Use of National Security Letters, please provide us with the following information (by close of business on April 4 if possible):

1) copies of all e-mails, memoranda, and other documents that relate to the F.B.I.'s use of "exigent letters," as well as transcripts of your interviews conducted on the issue.

2) please identify all of the F.B.I. personnel who participated in the creation and issuance of the "exigent letters."

3) copies of all documents, including internal memoranda, pertaining to the F.B.I.'s Communications Analysis Unit's contracts with the three telephone companies identified in the Inspector General's Report, and identify all F.B.I. attorneys who participated in the review and approval of those contracts.

4) copies of all documents pertaining to the information that the F.B.I. acquired through the use of National Security Letters (NSLs) pertaining to individuals who the F.B.I. concluded were irrelevant to terrorism investigations.

5) copies of all documents pertaining to the F.B.I.'s standards regarding the maintenance of the Office of General Counsel's National Security Letter database.

6) please detail the internal F.B.I. standards for the reporting of possible Intelligence Oversight Board violations, and provide any documents related thereto.

7) please identify F.B.I. standards pertaining to the review of investigative files to ensure that supervisory review of National Security Letter approval memoranda has occurred, and that the relevant authorizing statutes are in the NSLs.

8) copies of all internal communications relating to the F.B.I.'s use of Certificate Letters to obtain financial records from the Federal Reserve Bank.

9) please detail the F.B.I.'s reasons for the retention of data pertaining to individuals who the F.B.I. has concluded are irrelevant to terrorism investigations.

10) please explain why the F.B.I. had no policy or directive requiring the retention of signed copies of NSLs, or any requirement to upload NSLs in the F.B.I.'s case management system. Provide any documents relating to any decisions pertaining to this issue.

11) please detail why the F.B.I. does not have a uniform system for tracking responses to NSLs, either manually or electronically. Provide any documents relating to any decisions pertaining to this issue.

12) please detail why the F.B.I.'s database was unable to filter NSL requests for the same person in the same investigation.

13) please explain why the F.B.I. does not maintain records on NSL usefulness in criminal investigations and prosecutions.

Sincerely,

John Conyers, Jr.
Chairman

cc: Hon. Lamar S. Smith

PRESS RELEASE BY THE DEPARTMENT OF JUSTICE FROM MARCH 9, 2007, SUBMITTED BY THE HONORABLE HOWARD COBLE, A REPRESENATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA, AND MEMBER, COMMITTEE ON THE JUDICIARY

FOR IMMEDIATE RELEASE
FRIDAY, MARCH 9, 2007
WWW.USDOJ.GOV

AG
(202) 514-2008
TDD (202) 514-1888

FACT SHEET:
Department of Justice Actions on FBI Use of National Security Letters

WASHINGTON – The Attorney General commends the work of the Inspector General (IG) in uncovering serious problems in the FBI's use of National Security Letters (NSLs). The Attorney General has told the Director of the FBI that such mistakes will not be tolerated and has ordered the FBI and the Department to restore accountability and to put in place safeguards to ensure greater oversight and controls over the use of national security letters. The following are some of the actions directed by the Attorney General:

- The FBI Inspection Division will investigate the FBI's use of NSLs to determine management accountability.
- Although there has been no allegation of misconduct by FBI lawyers, the Attorney General asked the Associate Deputy Attorney General and the Office of Professional Responsibility to review the Inspector General's report and examine the role that the FBI lawyers played in the FBI's use of NSLs and exigent letters.
- The FBI has instituted new procedures to improve the handling of NSL records and increase training on the proper use of these letters.
- The Attorney General has directed the Justice Department's National Security Division (NSD) and Privacy and Civil Liberties Office to work with the FBI in implementing corrective actions, consider any further review and reforms that are needed, and to report to the Attorney General regularly on the process.
- The Attorney General has directed the NSD to begin oversight and auditing of the FBI's use of NSLs. The NSD, in conjunction with the FBI's inspection division, will conduct reviews of the use of NSLs in FBI headquarters and field offices. Any identified violations of law or guidelines will be reported to appropriate oversight authorities. This is a new level of oversight by Department of Justice lawyers with years of experience in intelligence and law enforcement.
- The Attorney General has ordered that briefings on the IG's report be given to the President's Foreign Intelligence Advisory Board, the Privacy and Civil Liberties Oversight Board, Congress, and key advocacy groups. Many of these briefings have already occurred.
- The Department and the Office of the Director of National Intelligence have established the NSL Data Retention Working Group, which is looking at how the Department retains the information it acquires.
- The Attorney General has directed the Department's legislative staff to review and revise as necessary the Department's responses to Congressional inquiries.
- The Attorney General has asked the Inspector General to report to him in four months on the FBI's implementation of the report's recommendations.

The Attorney General's Letter to the Inspector General

###

07-139

The Attorney General
Washington, D.C.

March 1, 2007

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

Dear Mr. Fine:

I appreciate your work and the opportunity to comment on your Review of the Federal Bureau of Investigation's Use of National Security Letters.

The problems identified in your review are serious and must be addressed immediately. I have spoken with FBI Director Bob Mueller about your findings and recommendations. He already has taken specific steps to correct past mistakes and to ensure that the Bureau will use National Security Letters (NSLs) in an appropriate manner in compliance with all applicable laws and internal policy requirements.

I have asked the Department's National Security Division and the Privacy and Civil Liberties Office to work with the Bureau in implementing these corrective actions and to consider any further review and reforms that are needed. They will report to me regularly on their progress. In addition, I ask that you report to me in four months on the FBI's implementation of your recommendations.

Your review also evaluated the effectiveness of NSLs and rightly found them to have "contributed significantly to many counterterrorism and counterintelligence investigations." NSLs are vital investigative tools and are critical to our efforts to fight and win the war on terror. They can and must be used appropriately and in a manner that protects the civil liberties of all Americans. I have confidence in the Director's ability to implement the changes necessary to ensure the proper use of these authorities.

Sincerely,

Alberto R. Gonzales

ARTICLE ENTITLED "OFFICIAL ALERTED F.B.I. TO RULES ABUSE 2 YEARS AGO, LAWYER SAYS," *THE NEW YORK TIMES,* SUBMITTED BY THE HONORABLE JOHN CONYERS, JR.

The New York Times

FROM DIRECTOR DANNY BOYLE

March 19, 2007

Official Alerted F.B.I. to Rules Abuse 2 Years Ago, Lawyer Says

By EDMUND L. ANDREWS

WASHINGTON, March 18 — Almost two years before the Federal Bureau of Investigation publicly admitted this month that it had ignored its own rules when demanding telephone and financial records about private citizens, a top official in that program warned the bureau about widespread lapses, his lawyer said on Sunday.

The official, Bassem Youssef, who is in charge of the bureau's Communications Analysis Unit, said he discovered frequent legal lapses and raised concerns with superiors soon after he was assigned to the unit in early 2005.

Stephen M. Kohn, the lawyer for Mr. Youssef, said his client told his superiors that the bureau had frequently failed to document an urgent national security need — proving "exigent circumstances," in the bureau's language — when obtaining personal information without a court order through the use of "national security letters."

Mr. Youssef said his superiors had initially minimized the scope of the problem and the likely violation of laws intended to protect privacy, Mr. Kohn said.

"He identified the problems in 2005, shortly after he became unit chief," Mr. Kohn said. "As in other matters, he was met with apathy and resistance."

Mr. Youssef's criticisms were first reported on Sunday by The Washington Post, which also cited internal e-mail messages in which Justice Department officials had discussed the legal lapses surrounding national security letters.

Mr. Youssef, born in Egypt, is suing the bureau for discrimination, charging that senior officials improperly suspected his loyalties in part because of his Egyptian origins.

On March 9, the inspector general for the Justice Department sharply criticized the F.B.I. over its heavy use of national security letters, saying it had found many instances in which the bureau had improperly and sometimes illegally used them to demand personal records from telephone companies, Internet service providers, credit companies and other businesses.

The report has provoked angry reactions from Republicans and Democrats in Congress, some of whom have charged that the bureau ran roughshod over civil liberties.

Unlike a search warrant, which must be approved by a judge, a national security letter can be approved by the agent in charge of a local F.B.I. office. The bureau has issued more than 20,000 such letters since it received authority under the antiterrorism law known as the USA Patriot Act of 2001.

One of the report's biggest criticisms was that top bureau officials signed off on many of the demands for information without properly justifying a specific national security need, like a clear link to a specific counterterrorism investigation. Mr. Kohn said that Mr. Youssef had had a long familiarity with national security letters from earlier work on counterterrorism investigations, and that he began reviewing recent letters and spotting legal deficiencies almost immediately.

"It was the same issue that was in the inspector general's report," Mr. Kohn said Sunday. "They didn't have the proper legal justifications in writing to back up their searches."

One of the F.B.I.'s few fluent Arabic speakers, Mr. Youssef won the Director of Central Intelligence Award in 1995 for his work infiltrating the Islamic group led by Sheik Omar Abdel Rahman, who is now serving a life sentence in prison on charges tied to the first bombing of the World Trade Center, in 1993. From 1996 to 2000, Mr. Youssef was the Justice's Department's legal attaché to Saudi Arabia, where he won praise for his work with Saudi officials on investigations of the bombing of the Khobar Towers in 1996.

Copyright 2007 The New York Times Company