A Review of the Federal Bureau of Investigation's Use of National Security Letters: *Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009*

Office of the Inspector General
Oversight and Review Division
August 2014

TABLE OF CONTENTS

TABLE OF FIGURES
[Table below is UNCLASSIFIED]

LIST OF ACRONYMS
[Table below is UNCLASSIFIED]

ACS	Automated Case Support
ADC	Assistant Division Counsel
ASAC	Assistant Special Agent in Charge
CAU	Communications Analysis Unit
CDC	Chief Division Counsel
CTD	Counterterrorism Division
CXS	Communication Exploitation Section
DIOG	Domestic Investigations and Operations Guide
DNI	Director of National Intelligence
ECPA	Electronic Communication Privacy Act
FBI OGC	FBI's Office of the General Counsel
FBI OPR	FBI's Office of Professional Responsibility
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FISA	Foreign Intelligence Surveillance Act
IOB	Intelligence Oversight Board
IP	Internet Protocol
JTTF	Joint Terrorism Task Force
LES	Law Enforcement Sensitive
NARA	National Archives and Records Administration
NSD	National Security Division
NSIG	National Security Investigation Guidelines
NSL I	Report in March 2007 covering calendar years 2003 through 2005, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*
NSL II	Report in March 2008 covering calendar year 2006, *A review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*
NSLB	FBI OGC's National Security Law Branch
NSL	National Security Letter
NSR	National Security Review
ODNI	Office of the Director of National Intelligence
OIC	FBI's Office of Integrity and Compliance
OIG	Department's Office of the Inspector General
OLC	Department's Office of Legal Counsel
OPR	FBI's Office of Professional Responsibility
PIOB	Potential Intelligence Oversight Board Violation
RFPA	Right to Financial Privacy Act
SAC	Special Agent in Charge
SSA	Supervisory Special Agent
TA	Telephone Application
TCAU	Telephonic Communications Analysis Unit
TFOS	Terrorist Financing Operations Section
XTS	Exploitation Threat Section (Section within the FBI's Counterterrorism Division)

EXECUTIVE SUMMARY

This Executive Summary summarizes the results of a follow-up review by the Department of Justice (Department) Office of the Inspector General (OIG) on the Federal Bureau of Investigation's (FBI) use of national security letters (NSL).[1] This review was initiated to evaluate the FBI's implementation of recommendations the OIG made in three prior reviews concerning the FBI's use of national security letters: *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, issued in March 2007; *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, Issued in March 2008, and *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records*, issued in January 2010.

In these three earlier reviews, the OIG found repeated instances of the FBI's misuse of NSL authorities during 2003 through 2006. We also discovered the FBI's practice of issuing exigent letters and using other informal methods to obtain telephone records, instead of using NSLs or

---

[1] The public version of this report contains redactions of information that the FBI determined is classified, law enforcement sensitive, or "for official use only."

In addition, the public version of this report contains several redactions of information that the FBI asserted is protected by the attorney-client privilege, attorney work-product doctrine, or deliberative process privilege. The classified version of this report provided to the Director of National Intelligence, the President's Intelligence Oversight Board, and Congress also contains redactions based on the FBI's assertion of the attorney-client privilege and attorney work-product doctrine. We disagree with those FBI assertions of attorney-client privilege, attorney work-product doctrine, and deliberative process privilege that have the effect of redacting types of information that were not redacted in the public and Congressional versions of our previous reports, such as guidance from FBI Headquarters to FBI field offices about whether certain information received by the FBI in response to an NSL may be kept and used by the FBI or whether the information is unauthorized and must be handled accordingly, and the reasons underlying the FBI's decision to not report certain matters to the Intelligence Oversight Board, a component of the President's Intelligence Advisory Board within the Executive Office of the President (PIAB).

Finally, during the sensitivity review of this report, the FBI provided a draft of the report to the PIAB, which asserted that certain information regarding guidance the Intelligence Oversight Board provided to the FBI on reporting intelligence oversight matters is "for official use only." We disagree with these markings, which have the effect of redacting information that we believe is important to the public's understanding of the FBI's compliance with NSL requirements. These markings have the further effect of redacting information in the public version of this report that is the same as or substantially similar to information that was included in the public versions of our previous reports.

other legal process. To address the findings in these reports, the OIG recommended that the FBI and the Department take specific corrective measures focused on creating new internal controls, providing guidance and training to FBI personnel, establishing new record-keeping practices, and conducting periodic reviews of NSL use. In addition, we recommended corrective measures to ensure that FBI personnel no longer use exigent letters or other informal methods to request and obtain telephone records, and to improve compliance with the statutes, guidelines, regulations, and policies governing the FBI's authority to request and obtain such records.

In this follow-up review, the OIG examined three topic areas. First, we assessed the current status of the FBI's and the Department's implementation of the recommendations made in our prior NSL reports, which covered the FBI's use of NSLs during calendar years 2003 through 2006. Second, we examined the FBI's use of NSLs during calendar years 2007, 2008, and 2009. This examination included an assessment of whether corrective measures taken by the FBI and the Department in response to the findings and recommendations of our first and second NSL reports resulted in improved compliance with NSL requirements. Third, we examined the current status of the FBI's and the Department's efforts to implement the recommendations made in our prior Exigent Letters Report.

To conduct the review, we examined over 15,000 documents, including internal policies and procedures, training materials, and guidance memoranda the FBI implemented after our earlier reports; memoranda from the FBI and the Department describing the status of their implementation of our recommendations; the Department's semiannual classified reports to Congress covering the FBI's use of NSLs in 2007 through 2011; documents reflecting potential NSL-related intelligence violations that FBI personnel self-reported to the FBI's Office of the General Counsel (FBI OGC) in 2008 and 2009 as well as the findings of numerous internal compliance reviews that the FBI and the NSD conducted during the same time period; and case files from two FBI field divisions. We also received a demonstration of the FBI's new NSL data system, known as the NSL subsystem to the Foreign Intelligence Surveillance Act Management System (NSL subsystem). We interviewed over 75 FBI and Department employees, including officials from the FBI OGC, Counterterrorism Division (CTD), and Inspection Division; personnel in 2 FBI field divisions; and officials from the Department's National Security Division (NSD).

I. Current Status of Implementation of Recommendations Made in the OIG's First and Second NSL Reports

We found that the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our past

reports and taking additional measures to improve the FBI's compliance with NSL requirements. In sum, we determined that the FBI and the Department have fully implemented 23 of 28 recommendations from our first and second NSL reports by creating new internal controls, providing guidance and training to FBI personnel, establishing new record-keeping practices, and conducting periodic reviews of NSL use.

We found that five recommendations require additional effort and attention from the FBI. For example, we found that the FBI's corrective measures have not completely eliminated potential intelligence violations resulting from typographical errors in the identification of a telephone number, e-mail address, or social security number in an NSL. These typographical errors cause the FBI to request and, in some instances receive, the information of someone other than the intended target of the NSL. We recommended that the FBI further reduce the risk of these violations by taking additional steps to improve the accuracy of information entered into the FBI's NSL subsystem.

We further found that additional effort from the FBI remains necessary to implement three recommendations we made in our previous reports to improve the FBI's record-keeping practices. To complete the implementation of two recommendations, the FBI should provide additional information and documents establishing that the FBI has considered, and will consider in the future, the feasibility of electronic tagging as it adopts new systems that process NSL-derived information. To fulfill the third recommendation, the FBI should provide additional guidance to the field to ensure that squad supervisors and agents verify adherence to NSL record-keeping requirements during quarterly case file reviews. We will consider whether to close these recommendations after the FBI provides additional information or takes the additional steps described in more detail in Chapter Two.

II. FBI's Use of National Security Letters during Calendar Years 2007, 2008, and 2009

As described in Chapter Three, our review found that during 2007 through 2009 the FBI issued significantly fewer NSL requests than during 2003 through 2006. The factors that may have contributed to the decrease in the FBI's NSL use during 2007 through 2009 are not self-evident from the data we reviewed, though a few people we interviewed at the FBI told us that because of increased scrutiny on NSL use, agents employed alternative investigative tools when possible. However, the Department's semiannual classified reports to Congress covering 2010 and 2011 indicate that the FBI's use of NSLs returned to historically typical numbers after 2009.

We found that the vast majority of NSL requests issued during 2007 through 2009 sought telephone and electronic records under Section 2709 of the *Electronic Communication Privacy Act* (ECPA). We also found that the FBI issued a majority of its NSL requests in furtherance of counterterrorism investigations and a significant number in furtherance of counterintelligence investigations. Well more than half of the FBI's NSL requests in 2007 through 2009 were generated from investigations of U.S. persons, indicating that the shift reported in our second NSL review toward more NSL requests generated from investigations of U.S. persons as compared to non-U.S. persons continued during this period.

With respect to the effectiveness of NSLs, our interviews of FBI Headquarters officials and field personnel, as well as our examination of case files and the FBI's data on NSL usage, showed that the NSL continued to be an important tool in the FBI's national security investigations conducted in 2007 through 2009. However, FBI personnel reported that beginning in 2009, certain Internet providers refused to provide electronic communication transactional records in response to ECPA NSLs. They reported that this refusal marked a change from past practice and has had a significant impact on the use and effectiveness of ECPA NSLs requesting such records. Consequently, [redacted].

Our compliance review of NSLs issued in 2008 and 2009 revealed that the corrective measures taken by the FBI and the Department in response to the findings and recommendations made in the OIG's first and second NSL reports resulted in substantial improvement in the FBI's compliance with NSL requirements. We believe that the substantial improvement is largely attributable to the FBI's implementation of the NSL subsystem. As described in Chapter Four, we found that the new NSL subsystem reduces opportunities for human error by including drop-down menus, limited choices, and self-populated fields. In addition, the subsystem's incorporation of ordered tasks and automated notifications helps to ensure that each NSL receives the required legal and supervisory review and approval. We also found that the FBI's mandatory training on NSL requirements and IOB reporting and new policies and procedures also contributed significantly to the FBI's improved compliance.

We identified ongoing compliance challenges in certain areas and made seven new recommendations to address those challenges. These new recommendations are intended to help improve: (1) case agents' adherence to the FBI's record-keeping practices; (2) their documentation of the relevance of each NSL request to the underlying investigation; (3) their identification of information received in response to an NSL that is beyond the scope of the NSL request; and (4) the FBI's substantial delays in

adjudicating potential intelligence violations, including those that require reporting to the President's Intelligence Oversight Board. The new recommendations also seek to address unauthorized collections, described in Chapter Four, involving [redacted] received in response to NSLs under the ECPA and personal consumer information received in response to NSLs under the *Fair Credit Reporting Act* (FCRA).

In our review, we encountered other noteworthy issues related to the FBI's use of NSLs, which we describe in Chapter Five. These issues include the scope of the term "toll billing records" in Section 2709 of the ECPA. We found that the FBI obtains many types of information in response to NSL requests for toll billing records, and it is unclear whether all of them fall within the scope of Section 2709. In particular, we concluded that the ECPA NSL statute does not clearly establish whether [redacted] obtained by the FBI's Telephonic Communications Analysis Unit (TCAU) – [redacted] – fall within the scope of toll billing records. Similarly, we concluded that although telephone carriers sometimes provided a social security number or date of birth in response to an NSL request for toll billing records, this information is not specifically enumerated in Section 2709 among the categories of information that the FBI may request or receive using an NSL.

To address these issues, we recommended that the Department revive its effort to bring about a legislative amendment to Section 2709 that more precisely defines the phrase "toll billing records." We believe the legislative proposal should clearly specify the categories of telephone and electronic records that the Department seeks to have Congress define as falling within the scope of ECPA Section 2709, in order to ensure that the FBI does not seek or obtain information to which it is not authorized. Because a legislative change may take time, we recommended that the Department should simultaneously seek a legal opinion from the Office of Legal Counsel as to whether the information described in Chapter Five and in the FBI's template attachment to ECPA NSLs falls within the scope of Section 2709.

We also identified an issue concerning the FBI's practice of requesting and receiving records "associated with" the records targeted in NSL requests. We believe that the plain language of the ECPA requires the FBI to first determine whether the records of a family member, business partner, or other individual associated with the account of the telephone number identified in an NSL are in fact relevant to a national security investigation before seeking such records directly through the NSL. We therefore recommended that the FBI take steps to ensure that FBI personnel do not request or obtain "associated" records without a separate determination and certification of relevance to an authorized national security investigation.

In addition, we identified an issue concerning the FBI's receipt of information in response to an NSL request after the authorizing investigation had closed or after the authority for the investigation had expired. We recommended that the FBI consider implementing a policy that would require agents, in consultation with OGC attorneys, to carefully balance the privacy interests of the individual against the potential for future investigative value before permitting the uploading into FBI databases of NSL return data received after a case has closed or after the authority for the investigation has expired.

III. Current Status of Implementation of Recommendations Made in the OIG's Exigent Letters Report

Finally, as described in Chapter Six, we found that the FBI and the Department have fully implemented 8 of 13 recommendations we made in our Exigent Letters Report to address the FBI's past use of exigent letters and other informal practices related to ECPA-protected telephone records. Five recommendations require additional effort and attention from the FBI or the Department. As to three of those recommendations, we found that the FBI should take additional steps to enhance its training and guidance on certain aspects of the ECPA.

In addition, we determined that the FBI should take further steps to address our recommendation concerning [redacted] of [redacted]. In our Exigent Letters Report, we found that the FBI conducted [redacted]. Because of the significant First Amendment interests implicated by such [redacted], as well as operational considerations such as obtaining cooperation from the media when necessary in future exceptional circumstances, we recommended that the Department re-evaluate the policies governing the conduct of [redacted] and consider under what circumstances FBI personnel may conduct [redacted], including whether approval by senior FBI officials at the level of an Assistant Director or higher should be required for the conduct of such [redacted].

Since that time, on July 12, 2013, the Department issued a report, *Report on Review of News Media Policies*, which made revisions to the Department's policies regarding investigations that involve members of the news media. Although this report did not specifically address [redacted], we believe the FBI should consult with the Department to determine whether the recent policy changes warrant any revisions to the DIOG's procedures for conducting [redacted] of members of the news media, including the approval level required before such [redacted] may be conducted.

The remaining recommendation in our Exigent Letters Report that is resolved but not closed concerns the FBI's [redacted], the U.S. Government may acquire:

[redacted].

The FBI reads [redacted] NSL statute, the [redacted].

The OIG's concern about this potential use was based on the fact that [redacted]. Since the issuance of the Exigent Letters Report, the OIG has requested information from the FBI and the Department about the FBI's use of the [redacted]. In June 2013, the Department informally told the OIG that the FBI [redacted]. On October 7, 2013, the Department stated in writing to the OIG that the FBI [redacted].

Meanwhile, the FBI has stated that its current policy in the DIOG is that the FBI may acquire telephone subscriber and transactional records as provided in Sections 2701-2712 of the ECPA, the provisions that require a government entity to obtain such records from a provider through legal process, or voluntarily if a provider in good faith believes that emergency circumstances warrant the disclosure. The FBI told the OIG that this policy [redacted] and those associated with [redacted]. The FBI also stated that [redacted]. However, we believe that FBI policy should more clearly state that FBI personnel should use Sections 2701-2712 of the ECPA to obtain telephone billing records for [redacted].

We will consider whether to close these recommendations after the FBI provides additional information or takes the additional steps described in more detail in Chapter Six.

IV. Conclusion

In sum, our review found that the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our past reports and taking additional measures to improve the FBI's compliance with NSL requirements. We found that the FBI fully implemented 31 of 41 recommendations from our first and second NSL reports and our Exigent Letters Report. Our review demonstrated that these efforts have resulted in substantial improvement in the FBI's compliance with NSL authorities. We found that 10 recommendations from our prior reports require additional information or attention, and we identify steps the FBI and the Department should take to address them. In addition, because we identified compliance challenges in certain areas, we made 10 new recommendations to the FBI and the Department to further improve the use and oversight of NSLs.

CHAPTER ONE
INTRODUCTION

This report is a follow-up to the first and second reports of the Department of Justice (Department) Office of the Inspector General (OIG) on the Federal Bureau of Investigation's (FBI) use of national security letters (NSL) after the enactment of the *USA Patriot Act* (Patriot Act) in 2001.[2] The first and second reports fulfilled a requirement in the *USA Patriot Act Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act) that directed the OIG to conduct reviews of the FBI's use of NSLs for two separate time periods.[3] The OIG issued its first report in March 2007 covering calendar years 2003 through 2005, *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, and its second report in March 2008 covering calendar year 2006, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006.* In these reviews, the OIG found repeated instances of the FBI's misuse of NSL authorities during 2003 through 2006. We also discovered the FBI's practice of issuing exigent letters and using other

---

[2] The public version of this report contains redactions of information that the FBI determined is classified, law enforcement sensitive, or "for official use only."

In addition, the public version of this report contains several redactions of information that the FBI asserted is protected by the attorney-client privilege, attorney work-product doctrine, or deliberative process privilege. The classified version of this report provided to the Director of National Intelligence, the President's Intelligence Oversight Board, and Congress also contains redactions based on the FBI's assertion of the attorney-client privilege and attorney work-product doctrine. We disagree with those FBI assertions of attorney-client privilege, attorney work-product doctrine, and deliberative process privilege that have the effect of redacting types of information that were not redacted in the public and Congressional versions of our previous reports, such as guidance from FBI Headquarters to FBI field offices about whether certain information received by the FBI in response to an NSL may be kept and used by the FBI or whether the information is unauthorized and must be handled accordingly, and the reasons underlying the FBI's decision to not report certain matters to the Intelligence Oversight Board, a component of the President's Intelligence Advisory Board within the Executive Office of the President (PIAB).

Finally, during the sensitivity review of this report, the FBI provided a draft of the report to the PIAB, which asserted that certain information regarding guidance the Intelligence Oversight Board provided to the FBI on reporting intelligence oversight matters is "for official use only." We disagree with these markings, which have the effect of redacting information that we believe is important to the public's understanding of the FBI's compliance with NSL requirements. These markings have the further effect of redacting information in the public version of this report that is the same as or substantially similar to information that was included in the public versions of our previous reports.

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

informal methods to obtain telephone records, instead of using NSLs or other legal process, and issued a separate report in January 2010, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records.*

To address the findings in these reports, the OIG recommended that the FBI and the Department take specific corrective measures focused on creating new internal controls, providing guidance and training to FBI personnel, establishing new record-keeping practices, and conducting periodic reviews of NSL usage. In addition, we recommended corrective measures to ensure that FBI personnel no longer use exigent letters or other informal methods to request and obtain telephone records, and to improve compliance with the statutes, guidelines, regulations, and policies governing the FBI's authority to request and obtain such records.

In this review, the OIG evaluated the FBI's and the Department's implementation of the recommendations made in our previous reports. We also examined the FBI's use of NSLs during calendar years 2007, 2008, and 2009. A primary focus of this examination was to assess the FBI's compliance with NSL requirements set forth in the NSL statutes, Attorney General Guidelines, and the FBI's internal policies following the corrective measures taken to address our previous findings.

I. The FBI's Authority to Issue National Security Letters

In our first NSL report, we described the background of national security letters and the four statutes authorizing the FBI to issue these letters to obtain non-content telephone and electronic communication records, financial records, and consumer credit information.[4] We briefly summarize those statutes and their requirements below.

National security letters are written directives to produce records that the FBI issues to third parties such as telephone companies, Internet service providers, financial institutions, and consumer credit reporting agencies. The *Electronic Communications Privacy Act* (ECPA), which principally affords federal privacy protections to telephone and other electronic communications, provides for the use of NSLs to obtain subscriber information and non-content transactional records relating to such communications in furtherance of national security investigations. 18 U.S.C. § 2709. The *Right to Financial Privacy Act* (RFPA), which affords federal privacy protections to consumer financial records, provides for the use of NSLs to obtain access to financial records in furtherance of national

[4] NSL I Report, 7-21.

security investigations. 12 U.S.C. § 3414. The *Fair Credit Reporting Act* (FCRA), which affords federal privacy protections to consumer information maintained by consumer credit reporting agencies, provides for the use of NSLs to obtain records relating to: (1) the identity of financial institutions with which a consumer maintains accounts and certain consumer-identifying information in furtherance of international terrorism investigations and clandestine intelligence activities ("FCRAu"), and (2) full consumer credit reports in furtherance of international terrorism investigations ("FCRAv"). 15 U.S.C. §§ 1681u and 1681v.[5]

Although the wording in the different NSL statutes varies, the central requirements are the same. First, each statute requires that the NSL contain a written certification. The ECPA, RFPA, and FCRAu NSL statutes require a certification that the requested records are relevant to or are being sought for an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution.[6] The FCRAv NSL statute requires a certification that the information is necessary for the investigation of, or intelligence or counterintelligence activity or analysis related to, international terrorism.[7]

Second, the ECPA, RFPA, and FCRAu NSL statutes require that the certification be signed by the FBI Director, or his designee in a position not lower than a Deputy Assistant Director at FBI Headquarters or a Special Agent in Charge of an FBI field division.[8] The FCRAv NSL statute requires that the certification be signed by a supervisory official designated by the FBI Director.[9]

Third, each NSL statute has special certification and notification requirements when the FBI invokes the statute's non-disclosure provisions. Each NSL statute permits the FBI Director, or the appropriate designee, to prohibit the recipient of an NSL from disclosing to any person that the FBI sought or obtained access to information under the NSL statute.[10] In order

---

[5] The *National Security Act*, which provides for the use of NSLs to obtain financial, consumer, and travel records of Executive Branch employees in furtherance of investigations involving suspected disclosure of classified information, is generally not used by the FBI and is not part of this review. 50 U.S.C. § 436.

[6] 18 U.S.C. § 2709(b), 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b).

[7] 15 U.S.C. § 1681v(a).

[8] 18 U.S.C. § 2709(b), 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b).

[9] 15 U.S.C. § 1681v(b).

[10] 18 U.S.C. § 2709(c), 12 U.S.C. § 3414(a)(5)(D), 15 U.S.C §§ 1681u(d) and 1681v(c).

to do so, the FBI Director or designee must certify in writing that such disclosure may result in a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person. In addition, the FBI must notify the NSL recipient of its non-disclosure obligations, including that: (1) the receipt of the NSL must remain confidential and cannot be disclosed except as required to comply with the NSL or obtain legal advice from an attorney; (2) if the recipient discloses the existence of the request to anyone (either to comply with the request or to obtain legal advice from an attorney), they must inform those individuals of the non-disclosure and confidentiality requirements; and (3) upon request of the FBI Director or his designees, the recipients must reveal the identities of the individuals to whom they disclosed the existence of the NSLs.[11]

Fourth, the NSL statutes require that the Department submit semiannual classified reports to Congress concerning all requests for information made under each of the NSL provisions.[12]

Finally, in addition to these requirements, the FBI's use of the NSL authorities, including the non-disclosure provisions, is now subject to several provisions in the Patriot Reauthorization Act relating to judicial review of NSLs. 18 U.S.C. § 3511.

In later chapters, we describe the statutory requirements for NSLs in more detail, as well as other relevant authorities set forth in Attorney

---

[11] Congress added these certification and notification requirements when it passed the Patriot Reauthorization Act. As originally drafted, the NSL statutes automatically imposed non-disclosure obligations on all NSL recipients, in perpetuity, without a mechanism for judicial review, and did not specifically allow recipients to disclose information as necessary to comply with the NSL request or to obtain legal advice from an attorney. Pub. L. No. 99-508 (1986), Pub. L. No. 95-630 (1978), Pub. L. No. 104-93 (1996). The non-disclosure provisions of the NSL statutes – both as originally drafted and as modified by the Patriot Reauthorization Act – have provoked significant public controversy and have been the subject of multiple judicial challenges. *See Doe* v. *Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (*Doe I*), *vacated and remanded by Doe* v. *Gonzales*, 449 F.3d 415 (2d Cir. 2006) and *Doe* v. *Gonzales*, 386 F. Supp. 2d 669 (D. Conn. 2005) (*Doe II*), *dismissed as moot, Doe* v. *Gonzales*, 449 F.3d 415 (2d Cir. 2006); see also *Doe* v. *Gonzales*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007) (after remand), *affirmed in part and reversed in part, Doe* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008). Most recently, the district court for the Northern District of California held the non-disclosure provisions in the ECPA NSL statute unconstitutional under the First Amendment. *In re National Security Letter*, 930 F. Supp.2d 1064 (N.D. Cal. 2013). The Department's appeal of this ruling is currently pending before the Ninth Circuit.

[12] 18 U.S.C. § 2709(e), 12 U.S.C. § 3414(a)(5)(C), 15 U.S.C. § 1681u(h), and 15 U.S.C. § 1681v(f).

General Guidelines, guidance from the President's Intelligence Oversight Board, and the FBI's internal policies.

II. Methodology of the OIG Review

In this follow-up review, the OIG examined three topic areas. First, we assessed the status of the FBI's and the Department's implementation of the recommendations made in our previous NSL reports concerning the FBI's use of NSLs during calendar years 2003 through 2006. To conduct this portion of the review, we evaluated memoranda from the FBI and the Department describing the status of the corrective measures they instituted to improve the FBI's compliance with law and policy governing the use of NSLs. We also reviewed internal policies and procedures, training materials, and guidance memoranda the FBI issued after our first and second NSL reports; and the written report and proposed procedures issued by a working group, known as the NSL Working Group, convened by the Department's Office of the Chief Privacy and Civil Liberties Officer and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence. We received a demonstration of the FBI's new NSL data system, known as the NSL subsystem to the Foreign Intelligence Surveillance Act Management System (NSL subsystem), described in more detail in the next chapter. In addition, we interviewed officials from FBI Headquarters, including the FBI's Office of the General Counsel (FBI OGC), Counterterrorism Division (CTD), and Inspection Division; and personnel in two FBI field divisions. We also interviewed officials from the Department's National Security Division (NSD).

Second, we examined the FBI's use of NSLs during calendar years 2007, 2008, and 2009 and the FBI's compliance with NSL requirements in 2008 and 2009 following the corrective measures taken to address our previous findings and recommendations. To evaluate the FBI's use of this tool during our review period, the OIG analyzed data contained in the Department's semiannual classified reports to Congress covering the FBI's use of NSLs in 2007 through 2009, as well as additional data derived from the FBI's new NSL subsystem. We also interviewed the FBI officials responsible for supervising and maintaining the NSL subsystem, and we interviewed personnel in two field divisions regarding the usefulness of the NSL as an investigative tool. To conduct the compliance portion of this OIG review, we analyzed the potential intelligence violations arising from the FBI's use of national security letters that FBI personnel self-reported to the FBI OGC in 2008 and 2009. We also examined the findings of numerous internal compliance reviews that the FBI and the NSD conducted during the same time period. As an additional measure of the FBI's compliance, we examined a judgmental sample of NSLs issued in 2008 and 2009 from two FBI field divisions, Boston and San Francisco. We also reviewed documents

provided by the FBI and the Department and interviewed officials from the FBI OGC, CTD, and Inspection Division, personnel in the two field divisions, and officials from the NSD.

The compliance review we conducted in the Boston and San Francisco Field Divisions included OIG investigators examining the records the FBI received in response to the NSLs in the judgmental sample to determine whether the FBI received information that was not requested or information that the FBI was not authorized to receive under the applicable authority. When OIG investigators from Washington, D.C., arrived at the FBI's San Francisco Field Division to begin reviewing investigative files, they were informed that they would not be permitted to review 12 credit reports the FBI received in a counterintelligence investigation in response to NSLs the FBI issued pursuant to Section 1681u of the FCRA because the FBI contended that Section 1681u(f) prevented the FBI from providing the OIG with access to those records. We were informed that the field division took this position based on guidance received from the FBI Office of General Counsel. As a consequence, the OIG's NSL team was initially prevented from reviewing 12 NSL returns containing credit report information the FBI obtained pursuant to Section 1681u and the integrity of the OIG's compliance review was put at risk. The OIG immediately notified the Office of the Deputy Attorney General of its objection to the FBI's position in light of the access provision in the Inspector General Act, and asked the Deputy Attorney General to direct the FBI to produce the credit report information to the OIG. The OIG was granted access to the material on the final day of its San Francisco site visit, but only after the Deputy Attorney General sent a letter to the FBI General Counsel and then-Acting Inspector General Cynthia Schnedar informing them that he had determined that disclosing the reports to the OIG in connection with the NSL review would be permitted pursuant to Section 1681u(f) because the Deputy Attorney General had determined that disclosure "was necessary to [his] informed decision-making regarding the approval and conduct of future foreign intelligence investigations."

The third topic area we examined was the FBI and the Department's efforts to implement the recommendations made in our Exigent Letters Report. To conduct this portion of the review, we examined relevant documents, including memoranda from the FBI and the Department describing the status of the corrective actions; documents from the FBI's Office of Professional Responsibility (OPR); and internal policies and procedures, training materials, and guidance memoranda the FBI issued after the OIG learned during our first NSL review of the FBI's practice of using exigent letters and other informal methods to obtain telephone records. We also interviewed FBI officials in the FBI OGC and Department officials from the NSD.

In sum, our review included interviews of over 75 FBI and Department employees and a review of over 15,000 documents.

III. Organization of this Report

This report is divided into seven chapters. Following this introduction, Chapter Two provides an overview of our previous findings and recommendations in our first and second NSL reports and assess the current status of the FBI's and the Department's efforts to address them.

Chapter Three describes the FBI's use of national security letters during calendar years 2007, 2008, and 2009. We present the FBI's data on NSL use and discuss the trends in the data from 2007 through 2009 and from 2003 through 2009. We also describe the usefulness of NSLs as an investigative tool and discuss a recent change in NSL use concerning electronic communication transactional records.

Chapter Four presents our findings regarding the FBI's compliance with NSL requirements set forth in the NSL statutes, Attorney General Guidelines, and the FBI's internal policies. We focused the compliance portion of our review on NSLs issued between January 1, 2008, and December 31, 2009, after the FBI's implementation of the NSL subsystem, described in Chapter Two, to generate and track NSL-related documents.

Chapter Five describes other noteworthy issues related to the FBI's use of national security letters that we encountered during our review.

Chapter Six provides an overview of our previous findings and recommendations in our Exigent Letters Report and describes and analyzes the FBI and the Department's implementation of the recommendations we made to address those findings.

Chapter Seven contains our conclusions and recommendations.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER TWO
STATUS OF THE FBI'S AND THE DEPARTMENT'S CORRECTIVE ACTIONS IN RESPONSE TO THE OIG'S FIRST AND SECOND NSL REPORTS

In our first NSL review we found widespread instances of the FBI's misuse of national security letters during 2003 through 2005.[13] We concluded that the widespread misuse was not the product of deliberate or intentional violations of law or policy but was instead due largely to inadequate guidance, training, and oversight regarding the use of these authorities. In addition, we discovered the FBI's practice of issuing exigent letters to obtain telephone records from three electronic communications service providers instead of using NSLs or other legal process. We concluded that this practice circumvented the requirements of the ECPA and violated the Attorney General's Guidelines and internal FBI policy. To address our findings, we made 11 recommendations to the FBI. In a letter to the Inspector General dated March 6, 2007, the Director of the FBI stated that the FBI agreed with all of the recommendations and would implement, and in some instances had already begun to implement, the recommended reforms.

In our second NSL review, we concluded that the FBI and the Department had made significant progress in implementing the recommendations contained in our first NSL report and in adopting other corrective measures to improve compliance.[14] We nevertheless found that additional work was needed to adequately address the problems and issues identified in our first and second reviews. Accordingly, we made 17 new recommendations to the FBI and the Department. In a letter to the Inspector General dated February 28, 2008, the Director of the FBI stated that the FBI agreed with all of the recommendations and had begun implementing them.

In this chapter, we describe the progress the FBI and the Department have made in implementing our recommendations since our second NSL report in March 2008. In Section I, we provide an overview of our previous findings and the corrective measures taken by the FBI and the Department in response to our prior reports. In Section II, we describe our specific recommendations and assess the current status of the FBI's and the

---

[13] NSL I Report, 67-108, 125-127.

[14] NSL II Report, 72-74, 160-64.

Department's efforts to implement them. In Section III, we set forth our conclusions and make further recommendations.

I. Overview of the OIG's Previous Findings and the FBI's and the Department's Corrective Measures

During our first NSL review, we found that the FBI's use of NSLs had grown dramatically following the enactment of the Patriot Act in October 2001.[15] We found that despite the increased reliance upon this important investigative tool, the FBI failed to provide clear guidance on the requirements and procedures for issuing NSLs to FBI personnel who conduct or provide operational support to national security investigations. We identified instances of improper or illegal use of NSL authorities and repeated failures to comply with internal FBI policies designed to ensure appropriate supervisory review of NSL use.[16]

The instances we identified of improper or illegal use of NSL authorities by field office personnel between 2003 through 2005 included:

- The issuance of NSL requests without proper authorization, caused by the failure to obtain the necessary approval from the Special Agent In Charge (SAC) or other authorized SES official or the failure to obtain required approval to extend the predicating investigation;
- The issuance of NSL requests seeking information outside the permissible scope of the NSL statute, including NSLs issued pursuant to the ECPA that sought prohibited content information and NSLs issued pursuant to Section 1681v of the FCRA that improperly sought full credit reports in counterintelligence cases;[17]

---

[15] NSL I Report, 121.

[16] NSL I Report, 67-108, 121-25.

[17] The original FCRA NSL statute, codified at 18 U.S.C. § 1681u, authorizes access in counterterrorism and counterintelligence investigations to consumer credit information limited to financial institution information and consumer identifying information. As part of the Patriot Act legislation, Congress enacted a new NSL authority in Section 1681v of the FCRA permitting the FBI to use national security letters to obtain full consumer credit reports in international terrorism investigations. This authority is limited to cases with a nexus to international terrorism. Section 1681v provides no authority to seek or obtain full credit reports in counterintelligence cases that have no nexus to international terrorism.

- The issuance of NSL requests relying upon the wrong statutory authority or failing to include the certification required by the applicable statute;[18]
- The issuance of NSL requests for the records of the wrong person caused by a typographical error in name, telephone number, account number, or other identifier in the NSL; and
- The receipt by the FBI of unauthorized information in response to an NSL, caused by a third party provider's error.[19]

In our first NSL review, we found one or more of these improper or illegal uses of NSL authorities in 22 percent of the case files we examined during our field visits. These matters should have been identified by the FBI and reported to the Intelligence Oversight Board (IOB) as potential intelligence violations but were not.[20]

In addition to these improper or illegal uses of NSL authority by field personnel, we found improper use of NSL authorities by units within the CTD at FBI Headquarters.[21] We determined that the FBI circumvented the requirements of the ECPA NSL statute by issuing so-called "exigent" letters to obtain telephone toll billing records and subscriber information from three telephone companies embedded within an operational support unit in CTD. We also determined that on 2 occasions CTD issued over 300 NSLs exclusively from so-called "control" files rather than investigative files in violation of FBI policy. We found that the use of "control files" rather than investigative files made it difficult or impossible to determine whether the

---

[18] Each NSL statute requires a specific written certification by the FBI Director or his designee. The certification, which is worded differently in each statute, confirms that the requirements of the applicable NSL statute have been met. In our first and second NSL reviews, we found instances where the FBI issued an NSL containing the wrong certification, such as an NSL requesting financial records pursuant to the RFPA NSL statute containing the certification required by the ECPA NSL statute.

[19] This report uses the term "unauthorized information" to describe information the FBI obtained from a third party provider that the provider was prohibited by statute to disclose to the FBI. This report uses the term "overcollection" to describe information obtained from a third party provider that is beyond the scope of an NSL request and the term "unauthorized collection" to describe overcollections that contain unauthorized information. Documents produced to the OIG in this review show that the FBI and the Department have most often used the term "overproduction" to describe overcollections and unauthorized collections. For consistency and clarity, in this report we use the terms "overcollection" and "unauthorized collection" rather than "overproduction."

[20] NSL I Report, 79-85. We describe the requirements and process for reporting possible intelligence violations to the IOB in Chapter Four.

[21] NSL I Report, 87-104.

NSL requests were tied to investigations that had the required evidentiary predicate for issuing NSLs.[22]

In 60 percent of the case files we examined, we found one or more failures to adhere to internal FBI policy regarding the documentation necessary for approval of NSLs.[23] These failures included:

- Electronic communications setting forth the basis and approval for the NSL request (approval ECs) that were not reviewed and initialed by one or more of the required field supervisors or Chief Division Counsel (CDC);
- NSL approval ECs that did not contain all of the required information; and
- NSLs that did not contain the certifications or other information required by the authorizing statutes.

While they did not rise to the level of potential intelligence violations, these compliance failures were violations of the FBI's internal control policies established to ensure the proper review, use, and tracking of NSLs.

Finally, we found that the electronic database used by the FBI OGC (OGC database) to track the FBI's use of NSLs and collect the NSL data necessary for congressional reporting was inaccurate and did not include information on all the NSL requests issued by the FBI.[24]

Accordingly, in our first NSL report, we made a total of 11 recommendations to the FBI to help improve its use and oversight of NSLs.[25] These recommendations focused on creating new internal controls, providing guidance and training to FBI personnel, establishing new record-keeping practices, and conducting periodic reviews of NSL usage. In response, the FBI and the Department took significant steps to address our recommendations and implemented additional corrective measures to improve NSL compliance and better track the FBI's use of NSLs. Our second NSL report described the actions taken by the FBI and the Department, which most notably included:

- The FBI Inspection Division conducted a large internal review, which included: (1) a random sample of 10 percent of the NSLs

---

[22] A "control file" is a term used by the FBI to describe an administrative or non-investigative file.

[23] NSL I Report, 104-08.

[24] NSL I Report, 31-36, 119-20.

[25] NSL I Report, 111-12, 126-27.

issued from the field during 2003 through 2006; (2) a random sample of 10 percent of the NSLs issued from FBI Headquarters during 2003 through 2006; and (3) a review of 100 percent of NSLs issued in counterintelligence cases pursuant to the FCRA during 2002 through 2006. The FBI's review confirmed the OIG's findings of widespread misuse of national security letters.[26]

- The FBI OGC issued a policy in March 2007 mandating that field offices conduct monthly counts of NSLs issued by their offices in order to reconcile NSL data contained in the OGC database. In April 2007, personnel in the FBI OGC instituted a process for comparing these monthly NSL counts to data in the OGC database to check for inaccuracies in the database.[27]
- Based on the OIG's findings, the FBI OGC issued additional guidance regarding the use of NSLs. Among other things, the new guidance directed FBI case agents to review records produced in response to NSLs prior to uploading the records into FBI databases to ensure that they correspond to requests in the NSLs and do not contain an overcollection. The guidance also prohibited the use of exigent letters; reiterated the distinctions between the NSL authorities in the FCRA; clarified the role of CDCs in conducting independent reviews of NSLs; and described procedures for redacting information received in response to but beyond the scope of NSLs, in order to prevent unauthorized dissemination. In June 2007, the FBI OGC issued a comprehensive 24-page memorandum setting forth FBI policy and guidance on the use of NSLs and NSL-derived information (Comprehensive NSL Guidance EC).[28]
- The FBI created a webpage on the FBI OGC's National Security Law Branch (NSLB) intranet site devoted to posting NSL-related guidance and information, including model approval ECs and NSLs.[29]
- The FBI OGC developed a new training module on NSLs incorporating the findings of the OIG's first NSL review, and conducted mandatory training in the field and at FBI

---

[26] NSL II Report, 75-103.

[27] NSL II Report, 20-21.

[28] NSL II Report, 17.

[29] NSL II Report, 38-39.

Headquarters for the Counterterrorism, Counterintelligence, and Cyber Divisions.[30]

- The FBI developed a new NSL data system to facilitate the issuance and tracking of NSLs. This new system, known as the NSL subsystem to the Foreign Intelligence Surveillance Act (FISA) Management System, is a web-based workflow that automates the generation and approval process for NSLs, as well as the collection of the data necessary for congressional reporting.[31]
- The FBI created a new Office of Integrity and Compliance (OIC) that reports to the Deputy Director. The mission of the OIC is to oversee a program that identifies compliance risks within FBI operations, develops compliance standards and training programs, and ensures that FBI activities are conducted in a manner consistent with laws, regulations, and policies.[32]
- The Department implemented national security reviews (NSR), a new compliance program for national security investigations in which teams of attorneys from the NSD and the NSLB review FBI case files for compliance with the requirements for the initiation, extension, and conversion of national security investigations, the issuance of NSLs and the handling of return data, and the reporting of violations to the IOB.
- The Department's Office of the Chief Privacy and Civil Liberties Officer and the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (ODNI) convened a working group, known as the NSL Working Group, to examine how NSL-derived information is used and retained by the FBI.

In our second NSL report, we concluded that the FBI and the Department had made significant progress in implementing the recommendations in our first NSL report and in adopting other corrective actions to address problems we and the FBI identified in the use of NSLs.[33] We also found that the FBI had devoted significant energy, time, and

---

[30] NSL II Report, 39-40.

[31] NSL II Report, 21.

[32] The OIC and the program it manages is described in more detail in the OIG's report, *Federal Bureau of Investigation's Integrity and Compliance Program* (November 2011), available at http://www.justice.gov/oig/reports/2011/e1201.pdf. In that report, we concluded that the FBI's OIC program had begun to reduce the FBI's risk of legal non-compliance in certain areas and had the potential to further reduce compliance risk through full implementation of its comprehensive mitigation plans.

[33] NSL II Report, 72-73.

resources toward ensuring that its field managers and agents understand the seriousness of the FBI's shortcomings in its use of NSLs and their responsibility for correcting these deficiencies.

However, because only one year had passed since our first NSL report, and some corrective measures had not been fully implemented, we stated in our second report that it was too early to definitely state whether the new systems and controls developed by the FBI and the Department had fully eliminated the problems with the use of NSLs that we identified.[34] Moreover, our second NSL report identified additional issues and made 17 new recommendations. These new recommendations were designed to focus the FBI and the Department's attention on ensuring the accuracy of information entered into the NSL subsystem; reinforcing NSL training and guidance, particularly with respect to FCRA NSLs; expanding periodic reviews, inspections, and oversight of the FBI's use of NSLs; and reexamining the FBI's policies on the retention and dissemination of NSL-derived information.

In Section II below, we provide updated information on the status of the FBI's implementation of the recommendations in our first and second NSL reports. Among the key measures taken by the FBI since the issuance of our second NSL report, the FBI:

- completed an audit of the OGC database and, in April 2010, submitted revised semiannual classified reports to Congress on the FBI's use of NSL authorities;
- fully implemented the NSL subsystem in all field divisions and FBI Headquarters and retired the OGC database;
- completed mandatory training in 2008 on NSL requirements and the NSL subsystem;
- issued the Domestic Investigations and Operations Guide (DIOG) in December 2008 and a revised DIOG in October 2011, which, among other things, incorporates and consolidates FBI policy and guidance on the use of NSLs and NSL-derived information;
- updated its IOB policy, which is available on the NSLB's intranet site, and completed mandatory training in 2008 and 2009 on the identification and reporting of potential IOB violations;

[34] NSL II Report, 161-63.

- conducted five internal compliance reviews of NSLs issued in 2008, 2009, 2010, 2011, and 2012; and
- conducted with NSD one or more NSRs of each FBI field division.

We concluded that these corrective measures, as well as other measures described below, demonstrate that the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our first and second NSL reports. In sum, we determined in this review that the FBI and the Department have fully implemented 23 of the 28 recommendations, collectively, by creating new internal controls, providing guidance and training to FBI personnel, establishing new record-keeping practices, and conducting periodic reviews of NSL usage. We believe that the implementation of these recommendations has contributed to the substantial improvement in NSL compliance that we describe in Chapter Four, and we consider these recommendations closed.

With respect to the remaining five recommendations, we concluded that the actions taken in response to the recommendations address but do not fully implement them, and thus that the recommendations are resolved but not closed. Once the FBI takes additional action or provides additional information, we will consider whether to close these recommendations.

II. Status of the FBI's and the Department's Implementation of the OIG's Recommendations

In this section, we organize our past recommendations into four broad categories: (1) internal controls, (2) guidance and training, (3) record-keeping, and (4) oversight. Within each category, we summarize each OIG recommendation and the corresponding response, and then provide the OIG's analysis. Where the FBI or Department has taken specific action on a recommendation that fully addresses the issue(s) the OIG identified, we consider the recommendation "closed." Where the FBI or the Department has taken specific action on a recommendation but we request additional action or information to address the issue(s) the OIG identified, we consider the recommendation "resolved" but not yet closed. Upon completion of the requested action or receipt of the requested information, we will consider whether to close the recommendation.

A. Internal Controls

Four recommendations in the OIG's first and second NSL reports were intended to improve the internal controls governing the creation and issuance of NSL requests to ensure that the requests meet NSL

requirements. As we discuss in detail below, we concluded that the FBI has fully implemented three of these recommendations, which we consider closed. One recommendation is resolved but remains open so that the FBI may consider an upgrade to the NSL subsystem to further address the recommendation.

Recommendation 8 (NSL I)
Status: Closed

OIG Recommendation: Given the widespread misuse of NSL authorities found during our first NSL review, we recommended that the FBI take steps to ensure that the FBI makes requests for information in accordance with the requirements of national security letter authorities.

Because some corrective measures taken by the FBI in response to the OIG's findings had not been fully implemented when we issued our second NSL report, this recommendation remained open after the OIG's second NSL report to give the FBI and the Department additional time to correct the problems we identified.

FBI Response: As described in Section I above, the FBI has taken several steps to improve the FBI's compliance with NSL authorities. Most importantly, the FBI: (1) developed and consolidated NSL policy and guidance in the Comprehensive NSL Guidance EC and the DIOG; (2) provided mandatory training to NSL users and approvers that explains and emphasizes this policy and guidance; (3) developed and implemented the NSL subsystem; and (4) conducted periodic inspections of NSL use through the FBI Inspection Division's NSL reviews and participated in the NSRs conducted jointly by the FBI and the NSD.

The NSL subsystem, in particular, significantly changed the FBI's work process for the creation and approval of NSLs. The NSL subsystem became fully operational on January 1, 2008, and, with limited exceptions, the FBI mandated that all Headquarters components and field offices use the subsystem to generate NSL requests.[35]

---

[35] The DIOG currently authorizes [redacted] to the mandatory subsystem requirement: (1) [redacted]

(Cont'd.)

The NSL subsystem is a computer program developed by the FBI to automate the creation and approval process for NSLs while simultaneously collecting the NSL data necessary for congressional reporting. When an authorized user, usually a case agent, initiates a new NSL request in the subsystem, the system prompts the user to complete all tasks necessary for the approval EC and the NSL. These tasks include specifying:

(1) [redacted];

(2) [redacted];

(3) [redacted];

(4) [redacted];

(5) [redacted];

(6) [redacted];

(7) [redacted];

(8) [redacted];

(9) [redacted];[36] and

[redacted].

[36] Each NSL statute requires that NSLs issued pursuant to that statute contain a written certification by the FBI Director or his designee that the requirements specified in the statute for compelling disclosure have been met. Each NSL statute also authorizes the FBI to impose non-disclosure obligations on the recipient of the NSL upon certification by the FBI Director or his designee that a specified harm may arise in the underlying investigation if disclosure of the NSL request occurs. When the FBI imposes non-disclosure obligations, the letter must notify the recipient of his non-disclosure obligations and, as of February 2009, his right to challenge the FBI's imposition of the non-disclosure requirement.

(10) [redacted].

The subsystem does not permit the case agent to move on to the next ordered task until the previous task has been completed.

Once the case agent completes all tasks, the subsystem prompts the agent to certify that the information sought is relevant to an authorized counterterrorism or counterintelligence investigation, that the authorization dates of the preliminary or full investigation have been correctly entered in the subsystem, and that the information in the NSL request is factually accurate.

The next several ordered tasks involve the review and approval of the NSL request by a Supervisory Special Agent (SSA) and an attorney (either division counsel in the field division or an NSLB attorney at FBI Headquarters), before final approval by an SAC or an Assistant Special Agent in Charge (ASAC) with final approval authority. The subsystem automates the approval process by sending an e-mail notification to the user responsible for completing the next approval.

Once final approval is granted, the subsystem generates the NSL with the information required by the relevant statute. The SAC or ASAC is responsible for signing the letter and forwarding the signed letter to the case agent who completes delivery of the NSL to the provider.

In addition to the features described above, the NSL subsystem is programmed to control for certain potential mistakes in the NSL process. For example, the subsystem is programmed to reject a control file number as the investigation case file number, and it will not accept a preliminary investigation with expired authorization dates. Moreover, many tasks in the subsystem include self-populated fields or provide drop-down menus or specific options for the case agent to choose from when completing a given task. These features are designed to ensure that, among other things, the FBI does not seek information not authorized by the statutory provision relied upon in the NSL. For example, a request for a full credit report under FRCAv is not an available option in a counterintelligence investigation. The subsystem is designed to recognize from the case file number entered into the system whether the case is a counterterrorism, counterintelligence, or cyber investigation and to filter the list of available NSL types to only those types permitted for that kind of investigation.

Because the circumstances of each investigation are unique, the NSL subsystem requires that the case agent describe the justifications for the investigation and the NSL request in free-text form. Drop-down menus, self-populated fields, and model language are not provided. Instead, the DIOG provides guidance regarding the justifications required for the

different types of NSLs. In addition, the NSL approvers review the stated justification and certify whether it is proper.

With respect to the non-disclosure provisions, the subsystem will prompt the case agent to choose whether to invoke the non-disclosure provisions and, if invoked, to either choose from a list of justifications (the same list of justifications explained in the DIOG) or to describe the justification in free-text form. If the NSL includes the non-disclosure provision, the letter will include a template paragraph describing the company's right to challenge the non-disclosure in district court. The FBI added this paragraph to its NSLs in February 2009 in response to *John Doe, Inc.* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008).[37]

Finally, the FBI recently updated its mandatory training courses on NSL requirements and the NSL subsystem. The FBI has stated an intention to require all NSL users to complete the updated training and thereafter retake the training every two years.

OIG Analysis: The FBI has taken appropriate steps to improve compliance with national security letter requirements. As we describe in more detail in Chapter Four, the corrective measures taken by the FBI and the Department in response to the findings in the OIG's first and second NSL reports have had a meaningful impact on the FBI's use of NSL authorities.

We found that the FBI's implementation of the NSL subsystem deserves much of the credit for the improvement demonstrated in 2008 and 2009. The NSL subsystem reduces opportunities for human error with drop-down menus, limited choices, and self-populated fields, and ordered tasks and automated notifications ensure that each NSL receives the required legal and supervisory review and approval.

---

[37] In *Doe* v. *Mukasey*, the plaintiffs challenged the constitutionality of the non-disclosure provisions of the NSL statutes, including new provisions passed in 2006 pertaining to judicial review. The Second Circuit held, among other things, that the non-disclosure provisions were unconstitutional to the extent they imposed a non-disclosure requirement upon an NSL recipient without placing the burden of initiating judicial review of the non-disclosure provisions upon the government. The court further held that in the absence of new legislation placing this burden on the government, the government could assume the burden on its own and adopt a "reciprocal notice procedure." Under this procedure, the government would be obligated to notify the NSL recipient of its opportunity to contest the non-disclosure requirement in the NSL and of its obligation to provide the government with prompt notice in the event it wishes to do so. Upon receiving notice of an NSL recipient's intent to contest the non-disclosure requirement, the government would then initiate litigation to enforce the non-disclosure provisions in the letter. *See* 549 F.3d at 883. As of this report, Congress has not enacted new legislation placing the burden of initiating judicial review upon the government.

At the same time, the NSL subsystem cannot eliminate FBI errors completely as it relies upon the careful entry of information provided by case agents and other FBI personnel with knowledge of the case file and NSL requirements. For this reason, we believe the FBI's mandatory training on NSL requirements and IOB reporting and the policies and procedures in the Comprehensive NSL Guidance EC and the DIOG, which have been explained and emphasized in the FBI's mandatory training, deserve considerable credit for the FBI's improved compliance described in Chapter Four. Finally, periodic inspections of NSL use and refresher training should help ensure that NSL users and approvers remain vigilant in their attention to NSL authorities and procedures and help to identify new or recurring compliance issues that can form the basis for additional guidance and compliance measures.

We therefore consider this recommendation closed. Although we identify later in this report certain issues that require additional information or improvement, we address those issues in other recommendations below and in new recommendations described in Chapters Four and Five.

Recommendation 3 (NSL II)
Status: Resolved

OIG Recommendation: In our first NSL review, we determined that the majority of the NSL-related potential intelligence violations in 2003 through 2005 resulted from FBI errors.[38] These errors included, among other things, the FBI issuing NSL requests containing a typographical error in the telephone number or e-mail address of the NSL target. The FBI commonly refers to this type of error as a "substantive" typographical error because the mistake in the telephone number, e-mail address, or other identifying information in the NSL substantively changes the target of the request from what was intended to an individual or account unrelated to the investigation.

In our second NSL report, we summarized the findings of the FBI's 2007 Field Review of NSLs and the findings of the first national security reviews conducted by NSD and FBI personnel in 2007.[39] We described how the findings were generally consistent with those identified in our first NSL report, including those regarding NSL requests containing substantive typographical errors. We also stated our expectation that the FBI's corrective measures in response to the findings of our first NSL review, namely the implementation of the NSL subsystem and the use of model NSL approval ECs and letters, would help reduce typographical and other data

[38] NSL I Report, 71-86.

[39] NSL II Report, 61-62, 81-85.

entry errors. However, we also noted that case agents and supervisors should still verify that the information relied upon in approval ECs and NSLs is accurately entered. Accordingly, we recommended in our second NSL report that the FBI implement measures to ensure that case agents or their supervisors verify that the identifying information contained in the NSL matches the identifying information contained in the source document in the case file.

FBI Response: The FBI responded that this recommendation has been addressed through training and the NSL subsystem. According to the FBI, it continues to train and advise its employees regarding their duty to accurately prepare NSLs and to verify critical data against authoritative documents to avoid clerical errors. A guidance document on the NSLB's intranet website entitled *NSL Review Checklist* reminds NSL drafters that typographical errors in NSL documents can lead to the collection of information not relevant to an investigation and further reminds them that they should double-check the accuracy of the information requested in the NSL.

With respect to the NSL subsystem, the FBI highlighted two features of the subsystem that it believes address this recommendation. The first is that the subsystem prompts the case agent generating the NSL to verify that the information in the request is factually accurate before the NSL may be approved. The second is that the NSL subsystem requires the case agent to enter the target's identifying information into the database only once, and then the subsystem populates that information into the NSL and approval EC from that same data entry point to ensure that the information is consistent.

OIG Analysis: As we describe in more detail in Chapter Four, the findings of our compliance review and the compliance reviews conducted by the FBI's Inspection Division and by the Department's NSRs of NSLs issued in 2008 and 2009 support the conclusion that the NSL subsystem has reduced human error in the creation of NSL requests. At the same time, the NSL subsystem cannot eliminate FBI errors completely and instead must rely upon the careful entry of accurate information.

We found during our compliance review described in Chapter Four that 21 of the 112 post-subsystem potential intelligence violations reported to the FBI OGC in 2008 and 2009 involved a substantive typographical error in an NSL caused by mistakes in the identification of a telephone number, e-mail address, or social security number for the target of the NSL. Most of these errors could have been prevented had the case agent generating the NSL carefully verified the telephone number, e-mail address, or social

security number using the relevant source documents in the case file.[40] To encourage this practice, we believe the certification requirement in the NSL subsystem should require the case agent to attest not only that the information contained in the request is factually accurate, but also that the information identifying the target (for example, telephone number, e-mail or IP address, social security number, or bank account number) has been verified with source documents in the case file.

In addition, although the entry of a target's identifying information into the NSL subsystem only once may help ensure consistency, it also perpetuates any data entry errors. For example, when the user makes a typographical error in the NSL target's telephone number, e-mail address, or social security number, the subsystem repeats that error as it populates the NSL and the approval EC with the same information. While many of these substantive typographical errors may be identified and corrected during the review and approval process, the potential IOB violations described in Chapter Four demonstrate that this is not always the case. Therefore, to further reduce substantive typographical errors, we believe the FBI should consider the efficacy of an upgrade that would require the user to enter the target's identifying information into the subsystem twice and not accept the information when the entries do not match.

Accordingly, we consider this recommendation resolved but not yet closed in order to give the FBI the opportunity to consider these upgrades or modifications of the NSL subsystem.

Recommendation 7 (NSL I)
Status: Closed

OIG Recommendation: During our first NSL review, we discovered the FBI's practice of issuing exigent letters to obtain telephone records from three electronic communications service providers instead of using NSLs or other legal process as required by the ECPA.[41] These exigent letters requested telephone records based on alleged "exigent circumstances," which in many cases did not exist and inaccurately stated that grand jury subpoenas or other legal process had already been sought for the records.

---

[40] In a few instances, the substantive typographical error appeared in the relevant source document that the case agent who initiated the NSL request relied upon.

[41] NSL I Report, 87-98. In our Exigent Letters Report issued in January 2010, we examined the use of exigent letters in depth. The report detailed how the FBI's practice of using exigent letters evolved, how widespread it became, and the management failures that allowed it to occur. The report also identified other informal methods used by the FBI to obtain telephone records without appropriate legal process and made additional recommendations to address the findings. We describe and analyze the status of those recommendations in Chapter Six of this report.

In some instances, there was no pending national security investigation associated with the requests at the time the exigent letters were issued. We concluded that by issuing exigent letters rather than NSLs or other legal process, the FBI circumvented the requirements of the ECPA and violated the Attorney General's Guidelines and internal FBI policy. Accordingly, we recommended that the FBI take steps to ensure that it does not improperly issue exigent letters.[42]

FBI Response: After our first NSL report, the FBI OGC sent several communications to FBI personnel stating that exigent letters are prohibited, and reiterated that instruction in mandatory NSL training. The FBI also clarified in guidance memoranda, and later in the DIOG and in the mandatory NSL training course in the FBI's Virtual Academy, the method by which FBI personnel may obtain certain non-content telephone and e-mail transactional data in emergency circumstances in accordance with authority in the ECPA at 18 U.S.C. § 2702(c)(4). The FBI has implemented an electronic form on the NSLB's intranet webpage to standardize the process of making Section 2702(c)(4) requests.

OIG Analysis: The FBI's prohibition of the use of exigent letters, along with its guidance and training on the requirements for obtaining certain non-content telephone and e-mail transactional data in emergency circumstances, address our recommendation, which we consider closed. The FBI must continue to emphasize in mandatory NSL training for all personnel assigned to national security investigations and to programs overseen by the National Security Branch that exigent letters and other circumventions of the NSL statutes are prohibited.

Recommendation 10 (NSL I)
Status: Closed

OIG Recommendation: In our first NSL report, we recommended that the FBI consider measures to ensure that CDCs and Assistant Division

[42] We also noted that the FBI General Counsel told us that the better practice, when exigent circumstances are present, 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. Section 2702(c)(4) provides an exception to the ECPA's prohibition against the disclosure to a government entity of non-content records pertaining to a subscriber or customer of a communications service provider. The exception requires that the provider has a good faith belief that an emergency involving danger of death or serious physical injury requires disclosure of the requested information without delay.

Counsel (ADC) in FBI field divisions provide close and independent review of requests to issue national security letters.[43]

FBI Response: On March 15, 2007, the FBI General Counsel held a conference call with all CDCs and on March 30, 2007, sent an e-mail to all CDCs and ADCs reminding them of the need to provide independent legal review of NSLs. In addition, the Comprehensive NSL Guidance EC mandates that CDCs and ADCs provide independent legal review of NSLs and provides the factors that they should consider before approving an NSL as legally sufficient.

OIG Analysis: We believe the FBI's actions emphasizing the importance of independent legal review of NSLs by CDCs and ADCs address this recommendation. During our field visits described in Chapter Four, we observed that the SACs, ASACs, supervisors, and case agents in the Boston and San Francisco Field Divisions relied upon their division counsel to provide thorough and independent legal review.

B. Guidance and Training

Ten of the recommendations in the OIG's first and second NSL reports were intended to improve guidance and training for FBI personnel on NSL requirements and the identification and reporting of potential intelligence violations to the FBI OGC. Overall, the FBI has taken considerable steps to address these recommendations and improve guidance and training on these issues. For the reasons discussed below, we conclude that the FBI has implemented all 10 of the recommendations, which we now consider closed.

Recommendation 4 (NSL I)
Status: Closed

OIG Recommendation: In our first NSL review, we found that FBI personnel responsible for issuing NSLs had significantly underreported potential IOB violations to the FBI OGC in 2003 through 2005.[44] We did not find that the underreporting of potential IOB violations was deliberate or intentional but instead concluded that a lack of guidance to assist FBI personnel in properly identifying such violations contributed to the high rate of underreported possible IOB violations we found. Accordingly, we recommended that the FBI consider issuing additional guidance to field divisions to assist them in identifying possible IOB violations arising from the use of national security letter authorities, such as guidance:

---

[43] NSL I Report, 126.

[44] NSL I Report, 79-86.

(1) identifying measures to reduce or eliminate typographical and other errors in NSLs so that the FBI does not collect unauthorized information; (2) addressing best practices for identifying the receipt of unauthorized information in responses to NSLs due to third party errors; (3) clarifying the distinctions between the two NSL authorities in the *Fair Credit Reporting Act* (15 U.S.C. §§ 1681u and 1681v); and (4) reinforcing internal FBI policy requiring that NSLs must be issued from investigative files, not from control files.

FBI Response: After our first NSL report, the FBI issued the Comprehensive NSL Guidance EC in June 2007 that, among other things, stated that the misuse of NSL authorities or NSL-derived information constitutes a potential IOB violation. The guidance identified four examples of violations that arise in the NSL context: (1) receiving information beyond the scope of an NSL request, regardless of whether FBI error or third party error caused the overcollection; (2) serving an NSL containing a substantive typographical error; (3) serving an NSL requesting information beyond the scope permitted by statute, such as content information or a full credit report in a counterintelligence investigation; and (4) failing to meet the statutory requirements for the issuance of an NSL, such as issuing an NSL in the absence of a preliminary or full national security investigation or failing to demonstrate the relevance of the requested information to the investigation.

In addition, the FBI implemented measures to reduce typographical and other errors in NSLs and approval ECs. The Comprehensive NSL Guidance EC mandated that FBI personnel use model NSLs and model approval ECs posted on NSLB's intranet webpage in the preparation of NSL documents. In January 2008, the FBI mandated use of the NSL subsystem to prepare NSL documents. As described under Recommendation 8 (NSL I) above, the subsystem was designed to improve compliance and minimize errors. To aid the preparation of NSLs that meet one of the narrow exceptions to the mandatory subsystem requirement, the FBI continued to maintain the model NSLs and approval ECs on NSLB's webpage.

To improve the handling of overcollections, the Comprehensive NSL Guidance EC mandated that case agents review NSL return data to ensure that the information received falls within the scope of the NSL request and did not include an overcollection. This guidance required that case agents conduct this review immediately upon receipt and before the information is uploaded into any database, and it provided instructions for the handling and reporting of overcollections.

The FBI also took steps to clarify the distinction between 15 U.S.C. § 1681u and 15 U.S.C. § 1681v of the FCRA. As described above in footnote 17, the original FCRA NSL statute, codified at 18 U.S.C. § 1681u (FCRAu),

authorizes access in counterterrorism and counterintelligence investigations to consumer credit information limited to financial institution information or consumer identifying information. As part of the Patriot Act legislation, Congress enacted a new NSL authority in Section 1681v of the FCRA (FCRAv) permitting the FBI to use national security letters to obtain full consumer credit reports in international terrorism investigations. This authority is limited to cases with a nexus to international terrorism. FCRAv provides no authority to seek or obtain full credit reports in counterintelligence cases that have no nexus to international terrorism.

In the OIG's first NSL review, we found that field personnel sometimes confused the two different authorities under the FCRA and requested or obtained consumers' full credit reports through NSLs issued pursuant to the FCRAv NSL authority in counterintelligence investigations unrelated to international terrorism. In response to this finding, the FBI issued a memorandum dated March 5, 2007, to all field offices and the FBI's Counterintelligence Division describing each of the FCRA NSL authorities and mandating that the components conduct a review of NSLs issued under the FCRA. The FBI repeated this guidance in the Comprehensive NSL Guidance EC and on the NSLB's intranet website. In addition, the FBI configured the NSL subsystem to disallow a request for a full credit report in a counterintelligence case.

To eliminate the issuance of NSLs from control files, the FBI issued a memorandum dated February 23, 2007, requiring that NSLs be issued from open investigative files and stating that the NSL approval EC must not refer solely to a control file number. The Comprehensive Guidance EC also prohibited the issuance of NSLs solely from a control file. In addition, the FBI configured the NSL subsystem to disallow the issuance of an NSL from a control file number.

In our second NSL report, we described the steps above and stated our expectation that they would assist FBI personnel in preventing and identifying potential IOB violations resulting from the use of NSL authorities. However, because our findings in the second NSL report identified certain problem areas that required greater emphasis and attention, we made new recommendations (Recommendations 10, 14, 15, and 16, discussed separately below) to help FBI personnel identify errors that constitute potential IOB violations – particularly errors involving FCRA NSLs – and improve the timeliness and consistency of field reports to the FBI OGC regarding potential IOB violations.

Following our second NSL report, the FBI took additional steps to implement Recommendation 4 in our first NSL report. The FBI provided training in 2008 and 2009 to all division counsel focused specifically on reducing, identifying, and reporting potential IOB violations. The training

covered the applicable NSL authorities, identifying potential IOB violations, the timing and content of reports notifying the FBI OGC of potential IOB violations, the identification and handling of overcollections, and specific factual examples of potential IOB violations that arise in the NSL context. All agents and supervisors assigned to national security investigations completed similar training. Further, for all current and new FBI employees, contractors, joint task force members, and detailees assigned to national security matters, the FBI required the completion of an on-line training course through the FBI's Virtual Academy on the identification and reporting of potential IOB violations within three months of the national security assignment.

In December 2008, the FBI issued the DIOG, which, among other things, incorporated policy and guidance from the Comprehensive NSL Guidance EC on the statutory requirements for NSLs (including the distinction between FCRAu and FCRAv) and the identification and handling of overcollections.

In April 2009, the FBI updated its IOB policy, *Guidance on Intelligence Oversight Board (IOB) Matters, Policy Implementation Guide.* The updated policy described the obligations and procedures for reporting potential IOB violations to the FBI OGC and provided eight specific examples of common NSL-related violations. [redacted], the policy also modified the circumstances under which FBI employees must report overcollections to the FBI OGC as potential IOB matters. The revised DIOG issued by the FBI in October 2011 incorporated the modifications set forth in the April 2009 IOB policy.

OIG Analysis: The FBI has taken substantial steps to assist field divisions in preventing, identifying, and reporting potential NSL-related IOB violations. As described in more detail in the next chapter, we found significant improvement in the FBI's compliance with NSL requirements in 2008 and 2009. At the same time, the FBI experienced a substantial increase in the reporting of potential IOB violations in 2007 through 2009, which we attribute in large part to the FBI's attention to and guidance on the obligation to closely scrutinize NSLs, examine information obtained in response to NSLs, and report potential violations to the FBI OGC. For these reasons, we consider this recommendation closed.

Recommendation 14 (NSL II)
Status: Closed

OIG Recommendation: In our second NSL review, we found that in 12 of the 34 potential intelligence violations reported by the FBI to the IOB in

2006 (35 percent), FBI personnel failed to report the matter to the FBI OGC in a timely fashion.[45] This finding related to events that preceded the issuance of the OIG's first NSL report in March 2007 and the FBI's corrective measures to address the findings in that report. As discussed above, after the issuance of our first NSL report, the FBI and other Department components took a variety of steps to promote compliance with NSL authorities and improve the identification and reporting of potential intelligence violations. In our second NSL report, we recommended that while these efforts were ongoing, the FBI should periodically reinforce in training and guidance provided to case agents and supervisors assigned to national security investigations the FBI OGC directive to report to the FBI OGC in a timely manner potential intelligence violations arising from the use of NSL authorities.

FBI Response: As described under Recommendation 4, above, the FBI provided training in 2008 and 2009 to all division counsel focused specifically on reducing, identifying, and reporting possible IOB violations. The training covered, among other things, the time requirements for reporting potential IOB violations to the FBI OGC. All agents and supervisors assigned to national security investigations completed similar training. Further, for all current and new FBI employees, contractors, joint task force members, and detailees newly assigned to national security matters, the FBI required the completion of an on-line training course through the FBI's Virtual Academy on the identification and reporting of potential IOB violations within three months of the new assignment.

The FBI does not mandate that FBI personnel complete a refresher course on potential IOB violations once the initial training requirement has been satisfied, but additional IOB guidance has been provided to the field during national security reviews and during annual legal training provided by each field division's CDC. The FBI OGC also requires all field divisions and relevant Headquarters components such as the Counterterrorism Division to certify on an annual basis that they have canvassed their employees and have no additional potential IOB violations to report to the FBI OGC. The annual canvass conducted in December 2012 included a reminder regarding the criteria and time requirement for reporting potential IOB violations to the FBI OGC.

OIG Analysis: The FBI's measures to reinforce training and guidance on potential IOB violations, including the time requirements for reporting potential IOB violations to the FBI OGC, satisfy this recommendation. The FBI should continue these measures, including the annual canvass, to keep

[45] NSL II Report, 143, 155.

attention on the requirement to report potential IOB violations. Accordingly, we consider this recommendation closed.

Recommendation 16 (NSL II)
Status: Closed

OIG Recommendation: To further improve compliance and the reporting of potential IOB violations to the FBI OGC, we recommended in our second NSL report that the FBI periodically provide case agents and supervisors assigned to national security investigations with examples of common errors in the use of NSLs, such as the examples used in its November 30, 2006, FBI OGC guidance memorandum regarding possible NSL-related intelligence violations.[46]

FBI Response: The FBI provided examples of common NSL-related errors in its Comprehensive NSL Guidance EC, its mandatory IOB training described above under Recommendations 4 (NSL I) and 14 (NSL II), and its April 2009 IOB policy. The FBI has also represented that it will continue the practice of incorporating anecdotal information regarding common errors in its NSL and IOB training and updating such examples as new issues arise.

OIG Analysis: The incorporation of practical guidance in IOB training should assist case agents and supervisors in their identification of potential IOB violations arising from their use of NSLs. As discussed in Chapter Four, the FBI OGC experienced a significant increase in the number of NSL-related potential IOB matters and third party overcollections reported by FBI personnel in 2007 through 2009, as compared to 2003 through 2006. We believe that this increase in reporting is largely attributable to the FBI's heightened awareness and oversight of its obligations to closely scrutinize NSLs for adherence to statutory requirements, examine information obtained in response to NSLs, and report potential violations to the FBI OGC. Accordingly, based on the steps the FBI has taken to improve compliance and the reporting of potential IOB violations, we are closing this recommendation.

Recommendations 7, 9, 10 (NSL II)
Status: Closed

OIG Recommendations: In our first NSL report, the OIG identified instances in which consumers' full credit reports were obtained or requested through an NSL issued pursuant to the FCRAv NSL authority in counterintelligence investigations unrelated to international terrorism, a

[46] NSL II Report, 156.

violation of the FCRAv NSL statute.[47] The FBI responded by undertaking a comprehensive review in 2007 of all such FCRA NSLs issued from January 1, 2002, through December 31, 2006. The objective of the review was to determine the extent to which NSLs relying upon FCRAv authority improperly requested or resulted in the receipt of consumer full credit reports in counterintelligence cases that had no nexus to international terrorism.

In our second NSL report, we summarized the findings of the FBI's 2007 FCRA NSL review, which confirmed that such violations of the FCRA statutory requirements had occurred.[48] In addition, we determined that the FBI's review demonstrated that because of confusion or a lack of knowledge about the statutory requirements, case agents, supervisors, CDCs, and SACs had failed to recognize that they had made improper requests under FCRA. Accordingly, we made three new recommendations to improve guidance and training on the distinction between the FBI's two NSL authorities pursuant to the FCRA. First, we recommended that the FBI reinforce the distinction between the two FCRA NSL authorities to all personnel in the FBI's National Security Branch at FBI Headquarters, in new agent training, in advanced training provided to agents and supervisors assigned to counterterrorism and counterintelligence programs, and in training provided to ASACs and SACs (Recommendation 7). Second, we recommended that the FBI reiterate in the FBI's continuing discussions with major credit reporting agencies that the agencies should not provide consumer full credit reports in response to FCRAu NSLs and should ensure that they provide only requested information in response to all FCRA NSLs (Recommendation 9). Finally, we recommended that the FBI ensure that guidance and training continue to identify the circumstances under which FCRA NSL matters must be reported to the FBI OGC as possible intelligence violations (Recommendation 10).

FBI Response: The FBI designed the NSL subsystem to disallow the issuance of FCRAv NSLs in investigations designated as counterintelligence investigations. The FBI also emphasized the distinction between FCRAu and FCRAv on the NSLB NSL webpage, in mandatory NSL and PIOB training provided to personnel who are assigned to national security matters, in the Comprehensive NSL Guidance EC, and in the DIOG. Further, the FBI added standard language to its FCRAu NSLs to ensure that consumer reporting agencies understand that the FBI is not requesting, and the agency should not provide, a full credit report in response to a FCRAu NSL requesting limited credit information. According to the FBI, the FBI has had

[47] NSL I Report, 71-72, 80-81.

[48] NSL II Report, 92, 101-102.

extensive discussions with consumer reporting agencies to ensure that they carefully review NSL requests and provide only the information requested in the NSL.

OIG Analysis: By providing the training and guidance described above to all FBI personnel assigned to national security investigations, the FBI has taken appropriate steps to ensure that FBI personnel assigned to national security investigations understand the distinction between the FCRAu and FCRAv NSL authorities and the circumstances under which improper use of these authorities can lead to potential IOB violations. The design of the NSL subsystem to disallow FCRAv NSL requests in counterintelligence investigations is another helpful measure to reinforce this distinction and ensure that the FBI uses its FCRAu and FCRAv authorities appropriately. We believe that training and guidance should continue in order to ensure that FBI personnel do not misuse FCRAu authority or fail to recognize that the receipt of a full credit report in response to a FCRAu NSL is improper and requires remedial action. Accordingly, Recommendations 7 and 10 (NSL II) are closed.

In addition, the FBI has taken appropriate steps to ensure that consumer reporting agencies understand the distinctions between FCRAu and FCRAv by addressing overcollection issues with the agencies and including standard language in FCRAu NSLs to remind them that the FBI is not requesting, and the agency should not provide, a full consumer credit report. Accordingly, Recommendation 9 (NSL II) is closed.

In closing these three recommendations, we are also informed by the results of our compliance review of NSLs issued in 2008 and 2009, discussed in Chapter Four, which found no instances of the FBI having requested or received a full credit report in a counterintelligence case.

Recommendation 15 (NSL II)
Status: Closed

OIG Recommendation: In our second NSL report, we recommended that the FBI require case agents and supervisors assigned to national security investigations to specify in any reports to the FBI OGC the precise remedial measures employed to handle any unauthorized information obtained in response to NSLs and to address whether the inappropriately provided information was used or uploaded into FBI databases.[49]

FBI Response: The FBI issued a new IOB policy in April 2009 that described the circumstances under which the receipt of information beyond

[49] NSL II Report, 163.

the scope of an NSL request should be reported to the FBI OGC as a potential IOB matter or as a third party error for tracking purposes only. The IOB policy set forth the specific information that must be included in the report, which includes [redacted].

To improve consistency and completeness in the reporting of potential IOB violations and overcollections, the FBI designed a new subsystem in its FISA Management System that provides an automated workflow for the preparation and submission of IOB reports and third party error notifications to the FBI OGC. An Assistant General Counsel in the FBI OGC who helps manage the FBI's IOB reporting told the OIG that the new IOB subsystem prompts FBI personnel to provide all the necessary information about the case file and the matter being reported, including whether any overcollected material was used or uploaded and whether any remedial measures have been taken, so that the FBI OGC can adjudicate matters without having to request additional information from the reporting office. According to the FBI, this IOB subsystem was implemented in all divisions on November 1, 2012.

OIG Analysis: Our review of potential IOB reports from 2007 through 2009 indicates that FBI personnel provided varying levels of information to the FBI OGC about the relevant investigation, the incident being reported, and whether any unauthorized collection was used or uploaded. The FBI developed a new subsystem to improve the reporting of potential IOB violations and any receipt of information outside the scope of the NSL request to the FBI OGC. The new IOB subsystem's automated workflow should help ensure the consistency and completeness of reports to the FBI OGC by prompting FBI personnel through each step of the reporting process. We therefore consider this recommendation closed.

Recommendation 13 (NSL II)
Status: Closed

OIG Recommendation: In our second NSL review, we examined a random sample of NSLs and approval ECs issued in 2006 to determine whether they complied with the non-disclosure requirements of the Patriot Reauthorization Act of 2005 and FBI policy.[50] Although we concluded that the vast majority of the NSLs and approval ECs we examined substantially complied with those authorities, we found that a small number of NSLs and

[50] NSL II Report, 117-30.

approval ECs did not. We found particularly troubling the failure of senior Counterterrorism Division officials to comply with the non-disclosure requirements in their issuance of so-called "blanket NSLs" in a failed attempt to remedy certain exigent letters issued in 2006. Accordingly, we recommended that the FBI periodically reissue guidance and training materials reminding case agents and supervisors assigned to national security investigations that they must carefully examine the circumstances surrounding the issuance of each NSL to determine whether there is adequate justification for imposing non-disclosure requirements on the NSL recipient.

FBI Response: The FBI's mandatory training on NSL requirements instructs national security personnel that when they are creating an NSL, the invocation of the non-disclosure provision should not be automatic and that a non-disclosure determination must be made on a case-by-case basis. The NSL subsystem reminds case agents of this instruction when they create an NSL and requires that the case agent choose from one of 13 possible non-disclosure justifications or provide a justification in free-text form before the subsystem will generate an NSL with the non-disclosure provision included. In addition, the DIOG and the model approval ECs on the NSLB intranet webpage require that the justification for the invocation of the non-disclosure provisions be set forth in the approval EC.

OIG Analysis: We believe that by reminding case agents that the non-disclosure provisions are not automatic and requiring case agents to provide justification when the provisions are invoked, the FBI's mandatory NSL training and the NSL subsystem help ensure that there is adequate justification for imposing non-disclosure requirements on NSL recipients. In addition, the DIOG and model approval ECs reinforce the requirement that approval ECs establish the justification for imposing non-disclosure. We therefore consider this recommendation closed.

Recommendation 11 (NSL I)
Status: Closed

OIG Recommendation: In our first NSL review, we recommended that the FBI provide guidance and training to special agents, CDCs, and all FBI officials authorized to sign NSLs regarding the meaning of the Attorney General's Guidelines' provision calling for use of the "least intrusive collection techniques feasible" and its application to the use of NSL authorities.[51]

[51] NSL I Report, 111

FBI Response: The Comprehensive NSL Guidance EC states that as part of their independent reviews of NSLs for legal sufficiency, CDCs, ADCs, or NSLB attorneys must not approve an NSL if a less intrusive means of obtaining the information is feasible. The FBI OGC also issued guidance dated December 20, 2007, to all divisions entitled "Least Intrusive Techniques in National Security and Criminal Investigations." This guidance identifies specific factors to be used to determine the intrusiveness of different investigatory methods and balance privacy and investigative interests. The FBI incorporated this guidance into the DIOG.

OIG Analysis: The Comprehensive NSL Guidance EC, the December 2007 guidance, and the DIOG appropriately emphasize the factors that agents must consider when they determine which investigative tools to use in their investigations. As described in Chapter Four, during our compliance review we asked several case agents and field supervisors on counterterrorism, counterintelligence, and cyberterrorism squads how they apply the least intrusive technique guidance to their use of NSLs. We generally found that case agents and supervisors understood the requirement to use the least intrusive method of investigation feasible. For example, many of them stated that they obtain and confirm relevant information through public sources and agency records before employing NSLs and other more intrusive investigative tools. Case agents, supervisors, and division counsel also described how they mitigate the intrusiveness of NSL requests by specifying date ranges for the requests in the letters and, when appropriate, seeking subscriber-only records to confirm the identity of the subscriber before seeking that subscriber's transactional records under the ECPA. Accordingly, this recommendation is closed.

Recommendation 5 (NSL I)
Status: Closed

OIG Recommendation: We found in our first NSL review that because the phrase "toll billing records" is not defined in the ECPA NSL statute, 18 U.S.C. § 2709, case agents and division counsel had questions about the types of information that can be obtained when making requests under this authority.[52] We also found that service providers produced different types of information in response to the FBI's requests for these records. Accordingly, we recommended that the FBI consider seeking a legislative amendment to the ECPA to define the phrase.

FBI Response: At the FBI's request, the Department drafted a proposed amendment to clarify the scope of the FBI's authority under

[52] NSL I Report, 112-13.

Section 2709.[53] The proposed amendment was sent to Congress on July 13, 2007, but was not enacted.

In addition, the FBI's General Counsel requested a legal opinion from the Department's Office of Legal Counsel (OLC) on the scope of the term "local and long distance toll billing records" in the ECPA NSL statute.[54] On November 5, 2008, the OLC issued its legal opinion concluding, among other things, that any call record that a communications provider keeps in the regular course of business and that could be used for billing a subscriber – even if not actually used for that purpose – falls within the scope of the ECPA NSL statute.

OIG Analysis: Because the Department proposed a legislative amendment to clarify the scope of the FBI's authority under Section 2709, we consider this recommendation closed.

However, as described in more detail in Chapter Five, uncertainty over the scope of the term "toll billing records" in Section 2709 remains. During our compliance review of NSLs issued in 2008 and 2009, we examined NSL return data that we believe raises new questions regarding the scope of the term "toll billing records" in the ECPA NSL statute, including whether [redacted] obtained by one of the FBI's operational support units falls within the scope of that term as interpreted by the OLC in its November 2008 opinion. We therefore make a new recommendation in Chapter Five that the Department continue its efforts toward a legislative amendment to the ECPA NSL statute and that any new proposal submitted by the Department address the questions we present in Chapter Five.

C. Record-keeping

The OIG made seven recommendations in its first two NSL reports that were intended to improve the FBI's record-keeping practices with respect to NSL-related information and the accuracy of NSL-related

---

[53] The proposed amendment would have authorized the FBI to obtain name, address, local and long distance connection records (or session times and durations), length and types of service, telephone or instrument number (or other subscriber number or identity, including any temporarily assigned network address), means and source of payment (including credit card or bank account number), and records identifying the origin, routing, or destination of electronic communications.

[54] Section 2709(a) states that a provider shall comply with a request for "subscriber information," "toll billing records information," and "electronic communication transactional records" under Section 2709(b). Section 2709(b)(1) allows the FBI Director or his designee to request "name, address, length of service, and local and long distance toll billing records." Thus, the "toll billing records information" that the FBI may request and that the provider must furnish is limited to "local and long distance toll billing records," also referred to in the statute and in this report as "toll billing records."

information submitted to Congress. For the reasons discussed below, we conclude that the FBI has implemented five of the recommendations, which we now consider closed. Two recommendations are resolved. We will consider closing these recommendations upon receipt of further information and documents from the FBI.

Recommendation 2 (NSL I)
Status: Closed

Recommendations 3 (NSL I) and 1 (NSL II)
Status: Closed

OIG Recommendations: In our first NSL review, the OIG determined that the database relied upon by the FBI OGC in preparing its semiannual classified reports to Congress did not contain accurate and complete information on NSL requests.[55]

Several problems affected the reliability of the FBI OGC database. First, we found that the FBI OGC database did not contain information on all NSLs issued by the FBI during the period 2003 through 2005.

Second, we found instances where the data fields in the FBI OGC database were left blank or contained typographical errors or other erroneous information. Default settings in the FBI OGC database caused some of the erroneous entries. For example, from 2003 through 2005, the database contained a default setting of "non-U.S. person" for the investigative subject. As a result, a U.S. person could be misidentified in the database if the default setting was not changed.

Other structural problems or flaws in the database resulted in discrepancies in the collation of data concerning the total number of NSL requests and total number of NSL targets during a given time period. We found that these problems caused significant inaccuracies and underreporting of NSLs and NSL requests to Congress, including the failure to report 4,600 NSL requests between 2003 and 2005 and the inaccurate reporting of the number of investigations relating to U.S. and non-U.S. persons.

Accordingly, in our first NSL report, we recommended that the FBI improve its database for tracking NSLs and NSL requests to ensure that it captures timely, complete, and accurate data (Recommendation 2).[56] In addition, because the FBI OGC database did not distinguish between the

---

[55] NSL I Report, 31-36, 121-122.

[56] NSL I Report, 119.

subject of an investigation and the target of an NSL, we recommended that the FBI OGC database capture data reflecting NSL requests for information about individuals who are not investigative subjects but are targets of NSL requests (Recommendation 3). Further, in our second NSL review, we recommended that the FBI create blank mandatory fields in the NSL subsystem (after it replaced the FBI OGC database) for entering the U.S. person/non-U.S. person status of the target of NSLs and for entering the number of NSL requests in order to prevent inaccuracies that may otherwise have resulted from the then-current default settings (Recommendation 1).[57]

FBI Response: As described above, the FBI developed an NSL subsystem in the FISA Management System, which replaced the previous FBI OGC database. In addition to providing an automated workflow for the generation and approval of NSL documents, the NSL subsystem is designed to automatically capture all of the data points necessary for congressional reporting. As case agents complete the web-based workflow to generate an NSL and approval EC, the subsystem prompts the agent to enter all of the necessary information for congressional reporting and then later uses a pre-defined reporting mechanism to compile the data points and provide the statistics given to Congress. These data points include the U.S. person status of the investigative subject and the target of the NSL request, and the number of NSL requests in each letter broken down by the U.S. person status of the NSL target.

The NSL subsystem became fully operational on January 1, 2008, and, with limited exceptions, the FBI mandated that all Headquarters components and field offices use the subsystem to generate NSL requests. For NSLs generated outside the subsystem (manually generated NSLs), case agents must send a lead that notifies the FBI OGC that a manually generated NSL has been issued and provides the FBI OGC with all the NSL data points necessary for congressional reporting.

After the issuance of our second NSL report, the FBI modified the NSL subsystem to remove default settings and instead require that case agents affirmatively select one of the U.S. person status options for the target of the NSL before the NSL may be approved.

OIG Analysis: In addition to reviewing the FBI's written responses to these recommendations, the OIG received a demonstration of the NSL subsystem and reviewed the data entries made in the subsystem for the NSLs we examined during our field visits. We found that the NSL subsystem has greatly improved the collection of NSL data for congressional reporting, particularly by sharply reducing opportunities for data entry

[57] NSL II Report, 23-24, 161.

errors and by immediately capturing the necessary data points as the NSL and approval EC are generated. These data points include the U.S. person status of the investigative subject and the target of the NSL request, and the number of NSL requests in each letter broken down by the U.S. person status of the NSL target. We therefore consider Recommendation 3 in our first NSL report and Recommendation 1 in our second NSL report closed.

Although we found that the NSL subsystem has greatly improved the collection of NSL data for congressional reporting, we note in Chapters Three and Four that the FBI's Inspection Division found during its review of NSLs issued in 2009 that the field failed to report to the FBI OGC [redacted] out of [redacted], or [redacted] percent, of the manually generated NSLs issued in that calendar year. Because timely reporting of manually generated NSLs to the FBI OGC is necessary to ensure that the NSL data reported to Congress is accurate, the reporting failures the FBI Inspection Division found mean that the Department failed to report these manually generated NSLs to Congress.

As described in Chapter Four, the FBI Inspection Division recommended that the FBI OGC reinforce training and guidance to ensure that divisions provide NSLB with the information regarding manually generated NSLs necessary for tracking purposes and congressional reporting. In response, the FBI included in the revised DIOG an e-mail address for reporting such matters to NSLB. The revised DIOG also clarifies the circumstances under which prior approval from NSLB is required and requires that the electronic communication authorizing the NSL provide the reason the NSL was generated outside the NSL subsystem and from whom approval was obtained. As described in Chapter Four, the FBI Inspection Division's most recent NSL reviews suggest that the measures the FBI has taken have improved compliance with the requirement to notify NSLB of manually generated NSLs. Further, the FBI has taken additional steps in response to the most recent NSL reviews to improve the tracking and reporting of manually generated NSLs. Accordingly, we consider Recommendation 2 (NSL I) closed.

Recommendation 1 (NSL I)
Status: Closed

Recommendation 11 (NSL II)
Status: Closed

OIG Recommendations: In our first NSL review, we learned that the FBI did not have a policy requiring the retention of signed copies of NSLs.[58] The unavailability of copies of the signed NSLs in specific cases made it

[58] NSL I Report, 27, 67.

impossible to determine whether NSLs were signed by the appropriate FBI officials or whether the issued letters contained the information required by the applicable NSL statute. We therefore recommended that the FBI require all personnel who are authorized to issue NSLs to maintain a control file for retaining signed copies of the letters (Recommendation 1).

In addition, in our second NSL review, we found a high percentage of instances in which information received in response to NSLs could not be located by FBI and OIG inspectors.[59] We therefore recommended that guidance should require that all NSL-derived information be appropriately documented, stored, easily identified, and readily available for internal and external review (Recommendation 11).

FBI Response: The Comprehensive NSL Guidance EC and the DIOG require that a copy of every signed NSL and the information received in response to the NSL be maintained in the investigative file. To further assist future audits, the FBI issued guidance in March 2008 requiring that hard copies of all signed NSLs, approval ECs, and records produced in response to an NSL be maintained in a "National Security Letter" sub-file in the investigative file. The NSL subsystem automatically uploads an unsigned electronic copy of the NSL and approval EC into the electronic case file in the FBI's Sentinel database, which recently replaced the FBI's Automated Case Support (ACS) database.

According to the FBI, the FBI's Inspection Division's internal compliance reviews of the FBI's use of NSLs in calendar years 2008, 2009, and 2010, described in more detail in Chapter Four, included an examination of whether signed copies of NSLs were forwarded to the relevant investigative case file. The written reports of these reviews, however, did not describe the results of these examinations.

OIG Analysis: The FBI issued policy and guidance requiring copies of all signed NSLs, approval ECs, and records produced in response to an NSL be maintained in an NSL sub-file in the investigative file. We believe that compliance with this requirement will assist future internal and external audits. Because the FBI issued the recommended policies, we consider our recommendations closed.

In Chapter Four, we make two new recommendations to improve compliance with the FBI's new record-keeping policies because we found during our compliance review that while the FBI had improved its record-keeping policies in 2008 and 2009, a significant number of NSL-related documents were nevertheless missing from the case files we reviewed. We

[59] NSL II Report, 102-03.

therefore recommend in Chapter Four that the FBI re-emphasize through additional guidance and training the importance of complying with the FBI's new record-keeping policies, including sending NSL-related documents, including NSL return data, to the appropriate NSL sub-file. We also recommend that the FBI monitor compliance with these policies during the FBI Inspection Division's NSL periodic reviews and report the results in the FBI Inspection Division's written reports.

Recommendation 6 (NSL I)
Status: Resolved

Recommendation 17 (NSL II)
Status: Resolved

OIG Recommendations: In our first NSL review, we found that the FBI generates a variety of analytical intelligence products using information derived from NSLs.[60] These products are stored in various FBI databases, shared within the Department and with Joint Terrorism Task Forces (JTTF), and disseminated to other federal agencies and members of the Intelligence Community. The FBI also provides information derived from NSLs to law enforcement authorities for use in criminal proceedings. However, because NSL-derived information is not marked, tagged, or otherwise identified as coming from NSLs when it is entered in FBI databases or when it is shared with law enforcement authorities or other Intelligence Community members, we found that it was impossible to determine when and how often the FBI provided NSL-derived information to law enforcement authorities for use in criminal proceedings (one of the topics the Patriot Reauthorization Act directed the OIG to address in our first two NSL reports). Accordingly, we recommended that the FBI consider measures to label or tag NSL-derived information so that the FBI's use of the information in intelligence products and in criminal proceedings can be better tracked.

In July 2007, at the direction of the Attorney General, the Department's Chief Privacy and Civil Liberties Officer convened an NSL Working Group to examine issues regarding how NSL-derived information is used, stored, and disseminated, with a particular focus on the retention of NSL-derived information.[61] Relevant to the recommendation we made in our first NSL review, in a draft memorandum to the Attorney General dated August 17, 2007, the NSL Working Group concluded that measures requiring tagging of NSL-derived information would place an undue burden

---

[60] NSL I Report, 52-65, 123, 126.

[61] The Working Group was chaired by the Department's Chief Privacy and Civil Liberties Office and included representatives from the FBI OGC, NSD, the Department's Office of Legal Policy, and the ODNI Office of the General Counsel.

on the use of NSLs. The group recommended instead that the FBI label all NSL-derived information and place the paper and electronic copies in an NSL sub-file within the investigative case file. In February 2008, the Privacy Officer told the OIG that the draft proposal had been withdrawn from the Office of the Attorney General so that the NSL Working Group could make enhancements to the proposal to describe more fully the research and findings of the Working Group and potentially strengthen its recommendations.

In our second NSL report, we analyzed the withdrawn proposal and offered comments for the NSL Working Group to consider as it re-examined important issues.[62] We concluded that the NSL Working Group's draft analysis of the tagging issue did not take into consideration the FBI's existing process for labeling NSL-derived information in the ACS and Telephone Applications (TA) databases, and whether that process can be adapted without undue burden and cost to follow NSL-derived information as it migrates to other databases and uses. We therefore recommended that the NSL Working Group, with the FBI's and NSD's participation, re-examine measures for (a) addressing privacy interests associated with NSL-derived information, including the benefits and feasibility of labeling and tagging NSL-derived information, and (b) minimizing the retention and dissemination of such information.

Response: In September 2010, the NSL Working Group issued a revised report with proposed procedures for the collection, use, and storage of NSL-derived information. The proposed procedures, which were approved by the Attorney General on October 1, 2010, provide steps that case agents and analysts should follow when they seek and after they obtain financial records, credit report information, electronic communication transactional records, and telephone subscriber and toll records through the use of an NSL. Although the procedures provide separate steps for each of these four categories of records, the commonalities among them are that the case agent or analyst should: (1) determine whether the NSL is the least intrusive means to obtain the information; (2) determine upon receipt of the information whether it is responsive to the NSL; (3) place all responsive documents in the NSL sub-file of the investigation hard-copy file, subject to the disposition schedule of the National Archives and Records Administration (NARA), and (4) record the receipt of the information in the electronic case file and upload it into applicable databases. In the case of [redacted] before including any items in analytical products or uploading any items into FBI databases.

[62] NSL II Report, 69-74, 163.

Relevant to the tagging issue, the NSL Working Group concluded that it would be prohibitively expensive to retrofit existing FBI systems to provide for electronic tagging. In support of its determination not to recommend electronic tagging, the Working Group further stated:

> The Working Group recognizes that electronic tagging may be the most efficient way to identify and remove NSL-derived information from FBI systems. It would also allow auditors to determine how often NSL-derived information is included in intelligence products or used in criminal investigations. The Working Group is not convinced, however, that learning the frequency with which NSL-derived information ends up in analytical products or criminal investigations would help determine anything of value, including whether NSLs were the "least intrusive collection technique feasible" in a given investigation. Because NSLs are frequently used to eliminate suspects and close leads, the relative absence [sic] of NSL-derived information in intelligence products and criminal investigations will not necessarily indicate that NSLs have been misused or overused. Nonetheless, because the Working Group believes tagging would facilitate the correction and removal of such information, it recommends incorporating the feasibility of electronic tagging into the Privacy Impact Assessments and IT system development processes the FBI uses when it adopts new case management and analytical systems that process NSL-derived information.
>
> The NSL Procedures [proposed by the NSL Working Group] provide a uniform method of segregating NSL-derived information from other investigative information in the hard copy and electronic case files. The FBI's existing systems are technologically capable of tracing the path of a particular piece of NSL-derived information back to its source. Although this practice does not confer the benefits of electronic tagging, the segregation of information would facilitate the retrieval, correction, and removal of information from the case files, when necessary.

In sum, the NSL Working Group recommended against adding electronic tagging to existing FBI systems because of the anticipated costs and what it perceived as limitations in the ability of electronic tagging to determine or measure the uses of NSL-derived information. Nevertheless, because electronic tagging would facilitate the correction and removal of such information when appropriate, the NSL Working Group recommended that the FBI consider the feasibility of electronic tagging as it adopts new systems that process NSL-derived information.

With respect to the existing system, the NSL Working Group found that the TA database has the capability to [redacted] as NSL-derived. The Working Group recommended implementation of this capability so that NSL-derived telephone numbers and subscriber information would be labeled as "NSL" in the TA database. The Working Group opined that such labeling would serve the same function as electronic tagging in that it would allow users and auditors easily to determine the source of, and remove, any data in the TA database improperly obtained through the use of NSLs.

With respect to the retention of NSL-derived information, the NSL Working Group recommended against using a retention protocol for NSL-derived information that would be shorter than the general retention protocol of 30 years for intelligence files and 20 years for criminal files in accordance with the NARA disposition schedule. The revised proposal relied upon the same reasoning as articulated in the prior proposal, that is, a shorter retention policy could undermine the integrity of the investigative file, and information gathered does not necessarily lose investigative value after the file is closed. The TA database has its own retention policy, and the Working Group recommended that the FBI evaluate the feasibility of limiting retention in that database by deleting telephone numbers that lose relevance and analytical value over time.

With respect to the dissemination of information outside the FBI, the NSL Working Group recommended that the FBI establish procedures to ensure that the dissemination of NSL-derived information to other federal agencies complies with Attorney General Guidelines as well as the restrictions imposed by federal statutes, but did not offer specific actions to help the FBI comply with those authorities. The Working Group did not recommend separate access restrictions on NSL-derived information on the ground that the sharing of information between the FBI and the Intelligence Community is important to their ability to "connect the dots."

According to the FBI, in response to the NSL Working Group's recommendations, the FBI implemented the recommended procedures by incorporating the following requirements into the revised DIOG:

(1) FBI personnel must use the least intrusive method to achieve investigative objectives;

(2) Before seeking to issue an NSL for [redacted], FBI personnel should [redacted] and whether an NSL is the "least intrusive and reasonable means" to obtain the information;

(3) [redacted]; and

(4) [redacted].

In addition, in response to the NSL Working Group's other recommendations, the FBI has represented to the OIG that the FBI: (1) will conduct Privacy Impact Assessments as necessary when adopting new FBI technologies and applications that will be used to store or analyze information received in response to NSLs; (2) implemented the electronic labeling feature in the TA database to identify information as NSL-derived; (3) evaluated the feasibility of limiting retention of NSL-derived information in the TA database and determined that retaining the information in a manner that differs from other telephone data is not feasible; and (4) incorporated in the revised DIOG the limitations on dissemination of information contained in the Attorney General's Guidelines and the restrictions on dissemination contained in the NSL statutes.

OIG Analysis: We believe the NSL Working Group's reexamination of the FBI's retention and dissemination policies and the FBI's incorporation of the Working Group's recommendations in the revised DIOG address the portion of Recommendation 17 (NSL II) concerning retention and dissemination of NSL-derived information. In addition, the NSL Working Group's reexamination of the feasibility of labeling and tagging NSL-derived information and the FBI's implementation of the labeling function in the TA database address in part the labeling and tagging issues identified in Recommendations 6 (NSL I) and 17 (NSL II). However, the FBI's stated intention to conduct Privacy Impact Assessments as necessary when adopting new FBI technologies and applications does not specifically include an intention to adopt the Working Group's recommendation that the FBI consider the feasibility of electronic tagging when developing new FBI technologies and applications. We therefore consider these recommendations resolved. We will consider closing these recommendations upon receipt of further information and documents from the FBI establishing that the FBI has considered, and will consider in the

future, the feasibility of electronic tagging as it adopts new systems that process NSL-derived information.

D. Oversight

The OIG made seven recommendations in its prior NSL reports that were intended to improve oversight of the FBI's use of NSL authorities. For the reasons discussed below, we conclude that the FBI has implemented five of the recommendations, which we now consider closed. Two recommendations are resolved but remain open for additional measures to be taken by the FBI and the Department.

Recommendations 4 and 8 (NSL II)
Status: Closed

Recommendation 12 (NSL II)
Status: Resolved

OIG Recommendations: In our second NSL report, we concluded that the FBI had made significant progress in addressing the compliance issues we identified during our first NSL review.[63] At the same time, we concluded that to ensure that NSL compliance remains embedded in FBI culture and practice, the FBI and the Department must be aggressive and vigilant in monitoring compliance with NSL statutes. Accordingly, we made several recommendations to assist the FBI and the Department in developing an effective oversight program for NSLs.

First, in Recommendation 4, we recommended that the FBI monitor the preparation of NSL-related documents and the handling of NSL-derived information with periodic reviews and inspections, including requiring that during quarterly file reviews squad supervisors conduct, at a minimum, spot checks of NSL-related documents in investigative files to ensure adherence to NSL authorities, Attorney General Guidelines, and internal FBI policies governing use of NSL authorities. Second, in Recommendation 8, we recommended that the FBI Inspection Division's periodic reviews and the NSD's national security reviews include review of the use of FCRA NSLs in counterintelligence investigations. Finally, in Recommendation 12, we recommended that the FBI's routine case file reviews and the NSD's national security reviews include an analysis of the FBI's compliance with requirements governing the filing and retention of NSL-derived information.

FBI Response: Following our second NSL report, the FBI's Inspection Division conducted five separate reviews of the FBI's compliance with NSL

[63] NSL II Report, 49, 162-63.

authorities – the first covering calendar year 2008 ("2008 review"), the second covering calendar year 2009 ("2009 review"), the third covering the first half of calendar year 2010 ("2010 review"), the fourth covering the second half of calendar year 2010 and the entire calendar year 2011 ("2010-2011 review"), and the most recent covering calendar year 2012 ("2012 review"). In addition, in April 2007, the Department initiated its NSR program to examine, among other things, the FBI's compliance with NSL authorities. Through this program, teams of attorneys from NSD and the FBI OGC visit 15 to 18 field divisions each year and review FBI case files for compliance with the requirements for the issuance of NSLs and the handling of return data, among other requirements.[64]

The FBI told the OIG that because of the periodic NSL reviews conducted by the FBI Inspection Division, and because the NSL subsystem requires specific reviews and certifications during the approval process, the FBI decided not to mandate spot checks of NSLs during quarterly case file reviews performed by squad supervisors. The FBI reasoned that spot checks would provide little value because they would require supervisors to re-check NSLs that they have already reviewed and approved.

With respect to the inclusion of FCRA NSLs in the FBI Inspection Division's periodic reviews, the 2008, 2009, and 2010 reviews included examinations of all FCRA NSLs issued by the FBI components audited. The 2010-2011 review included an examination of all FCRA NSLs issued by the Counterintelligence Division, and the 2012 review included an examination of FCRA NSLs in its random sampling. Further, as reflected in the NSD's written reports, FCRA NSLs issued by the FBI's field divisions are examined during periodic NSRs.

With respect to periodic reviews of the FBI's compliance with the requirements governing the filing and retention of NSL-derived information, the FBI states that it now requires supervisors to examine compliance with these requirements during quarterly case file reviews and that it documented this requirement in the DIOG. In addition, during NSRs conducted between 2007 through 2009, the review teams examined whether a signed copy of the NSL and the records produced in response are in the appropriate investigative file. The NSRs also examined the actions taken by the FBI to address any unauthorized information received in response to an NSL.

OIG Analysis: The FBI and the Department have devoted considerable resources to conducting periodic reviews of the FBI's NSL use.

---

[64] The NSL-related findings made in the NSRs between 2007 and 2009 are described in Chapter Four.

We believe the reviews are necessary to ensure that FBI personnel remain vigilant in their adherence to NSL authorities and procedures. These periodic reviews also provide considerable value in terms of identifying new or reoccurring compliance issues that can form the basis for additional guidance and compliance measures. We therefore consider Recommendation 4 closed. In addition, because the FBI Inspection Division's NSL reviews include a 100 percent inspection of FCRA NSLs, and because FCRA NSLs are also examined during NSRs, we consider Recommendation 8 closed.

As described more fully in Chapter Four, we found that while the FBI Inspection Division's NSL reviews addressed the FBI's compliance with NSL authorities in many important respects, the written reports did not address two significant data points – the extent to which the inspectors found NSL documents in the appropriate NSL sub-file, and the extent to which they found that the FBI appropriately remedied unauthorized collections caused by third party error. As a result, we believe the reviews conducted by the FBI Inspection Division should be expanded to measure: (1) the extent to which NSL-related documents are found in the appropriate NSL sub-file; and (2) with respect to unauthorized collections caused by third party error, the extent to which case agents identified and sequestered the unauthorized collection and either redacted, returned, or destroyed the information. We make a new recommendation at the end of Chapter Four to address these issues.

With respect to monitoring the FBI's compliance with filing and retention requirements for NSL-related documents, we believe the requirement that supervisors examine these issues during quarterly case file reviews should help improve compliance with the FBI's filing and retention policies. A few of the field supervisors we interviewed during our compliance review, however, told us that they did not routinely conduct this examination during quarterly case file reviews. Two of them also told us that checking whether NSL-related documents are in the appropriate NSL sub-file is not one of the purposes of quarterly case file reviews. The revised DIOG provides that supervisors should consider during file reviews whether NSLs, if any, have been issued in accordance with NSL policy, including whether NSL return data has been reviewed for overcollection. The revised DIOG does not state that supervisors should ensure that NSL-related documents are in the appropriate NSL sub-file. Accordingly, we believe the FBI should consider providing additional guidance to the field to ensure compliance with this requirement and revising the template for the case file review reports to have each case agent state whether all NSL-related documents are in the NSL sub-file. We therefore consider Recommendation 12 resolved but not yet closed.

Recommendation 2 (NSL II)
Status: Resolved

OIG Recommendation: In our first NSL report, we described how the FBI collected data on NSL usage by relying upon support staff in the FBI OGC to manually record NSL-related information.[65] We found that mistakes made by FBI personnel in entering NSL data into the FBI OGC database affected the accuracy of the database and contributed to inaccuracies in the Department's reports to Congress. During our second NSL review, the FBI stated that additional training provided to personnel performing data entry and the implementation of the then-new NSL subsystem would improve the timely, complete, and accurate collection of NSL data.[66] However, to ensure that training and the NSL subsystem eliminated or reduced data entry errors, we recommended that the FBI include periodic reviews of a sample of NSLs in the NSL subsystem. We said that these periodic reviews should draw upon resources available from the FBI Inspection Division and the FBI's new Office of Integrity and Compliance (OIC).

FBI Response: The FBI has represented that this recommendation was "largely superseded" by full implementation of the NSL subsystem because the NSL data upon which congressional reports are drawn is recorded in the subsystem as NSLs are created, rather than in the former database that relied upon data entry by support staff.

OIG Analysis: As we describe in Chapters Three and Four, the NSL subsystem has substantially reduced opportunities for human error by automatically capturing all of the data points necessary for congressional reporting. This function of the subsystem has eliminated reliance upon support staff in the FBI OGC to manually record NSL-related information, with the exception of the relatively small number of manually generated NSLs, which require physical entry of the congressional data points in the NSL subsystem.

Nevertheless, as we note throughout this report, the NSL subsystem cannot eliminate FBI errors completely and instead must rely upon the careful entry of accurate information. It is still necessary, for example, that a case agent enters the correct U.S. person status of the investigative subject and NSL target when generating an NSL in the subsystem. We continue to believe the FBI should consider incorporating in the FBI Inspection Division's NSL reviews an examination of a sample of the data entries made in the NSL subsystem, including the entries made in connection with manually generated NSLs, to evaluate and help ensure the

---

[65] NSL I Report, 32-34.

[66] NSL II Report, 20-23.

accuracy of the information entered into the subsystem. Accordingly, this recommendation is resolved but remains open so that the FBI may provide additional information or take additional steps to address this recommendation.

Recommendations 9 (NSL I) and 5 (NSL II)
Status: Closed

OIG Recommendation: In our first NSL review, we noted our concern that NSLB attorneys did not have accurate and complete information about the FBI's use of NSL authorities.[67] We found that NSLB attorneys were not consulted in advance about investigative tools used by the FBI Headquarters' National Security Branch, including the use of exigent letters by the Communications Analysis Unit (CAU) in the Communications Exploitation Section of the Counterterrorism Division to obtain ECPA-protected information, the use of so-called certificate letters by the Terrorist Financing Operations Section (TFOS) to obtain RFPA-protected information, and the use of control files rather than investigative files as the predicate for NSLs. Accordingly, in our first NSL report, we recommended that the FBI implement measures to ensure that the FBI OGC is consulted about activities undertaken by the National Security Branch, including operational support activities that could generate requests for records from third parties that the FBI is authorized to obtain exclusively through the use of its NSL authorities.

In our second NSL report, we noted that the FBI mandated in 2007 that NSLB attorneys involved in national security law matters review and approve all NSLs issued by FBI Headquarters and regularly attend certain operational meetings to provide legal advice and oversight.[68] According to the FBI, attorneys in the NSLB's two operational units began regularly attending operational meetings of the CAU, the Electronic Surveillance Operations and Sharing Unit, and the Communication Exploitation Section at Headquarters. The NSLB attorneys that provide legal advice to counterintelligence operations also began regularly attending operational meetings to play a more active legal role. In addition, the FBI represented that the NSLB Unit Chiefs regularly attend operational meetings and have daily contact with their units to provide legal advice, to spot legal issues, and to provide guidance and oversight on national security matters, including NSLs. The NSLB also assigned an NSLB attorney to each of two large field offices, New York and Los Angeles, to support the national security law program in those offices. Finally, NSLB attorneys also have

[67] NSL I Report, 87-103.

[68] NSL II Report, 42-44.

provided NSL training to operational units in the Counterterrorism and Counterintelligence Divisions.

While we concluded in our second NSL report that these measures should help ensure that FBI OGC attorneys are consulted about operational activities, we recommended that the FBI have NSLB attorneys participate in the operational meetings of the other units of the Counterterrorism and Counterintelligence Divisions to make sure the FBI OGC is in a position to identify and address improper requests for information. In response to this recommendation, the FBI stated that the "NSLB has continued the well-established practice of requiring attorneys to attend these meetings."

FBI Response: According to the FBI, three of the NSLB's four "Law Operations" units directly support the operational activities of the Counterterrorism Division and the other directly supports the Counterintelligence Division. As part of this direct support, each of these units is responsible for: (1) reviewing operational communications for legal sufficiency and compliance; (2) providing advice when intelligence, national security, or U.S. person information is disseminated or requested; (3) assisting domestic and foreign prosecutions; and (4) reviewing a wide variety of operational documents in counterterrorism and counterintelligence cases, including NSLs issued by Headquarters components. Attorneys from these units participate in regularly scheduled unit meetings and in meetings at which operational plans and details in particular matters are discussed. In addition, the Section Chief of the Operational Support Section and the Law Operations Unit Chiefs attend daily operational briefings with Counterterrorism and Counterintelligence Division management.

During an interview with the OIG, Steven Siegel, the former Deputy General Counsel of the FBI OGC in charge of NSLB between September 2009 and April 2012, told us that NSLB attorneys generally support all of the operational units in the Counterterrorism Division, but because of resource issues, NSLB was unable to assign an NSLB attorney to each unit. Siegel told us nevertheless that NSLB attorneys and supervisors collectively cover the unit and section meetings within the Counterterrorism Division.

OIG Analysis: We believe that regular participation by NSLB attorneys and supervisors in the unit and section meetings within the Counterterrorism and Counterintelligence Divisions, and the review of operational communications and documents for legal sufficiency and compliance, are important steps to help ensure that FBI OGC attorneys are aware of and consulted about operational activities. We therefore consider these recommendations closed.

Recommendation 6 (NSL II)
Status: Closed

In July 2007, the FBI announced the creation of the Office of Integrity and Compliance with the stated mission of ensuring there are processes and procedures in place that promote FBI compliance with the letter and spirit of all applicable laws, regulations, and policies. In our second NSL report, we recommended that the FBI consider increasing the staffing level of its newly formed OIC so that it can develop sufficient skills, knowledge, and independence to lead or directly carry out critical elements of its work. The OIG described the work of the OIC in a separate report issued in November 2011 entitled, *Federal Bureau of Investigation's Integrity and Compliance Program*, available at www.justice.gov/oig/reports/2011/e1201.pdf. In that report, the OIG found that the OIC, through the integrity and compliance program it manages, identified potential compliance risks within the FBI, developed mitigation plans for 13 compliance risks and, as of August 2011, implemented strategies that reduced compliance risk in 3 areas. The OIG also found that the OIC enhanced the FBI's ethics program by establishing initiatives to encourage compliance and ethical behavior within the FBI. In addition, the OIG made recommendations to help increase the effectiveness of the OIC. Based on these findings and recommendations, we consider Recommendation 6 from our second NSL report closed.

III. Conclusions and Recommendations

The corrective measures described above demonstrate that the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our first and second NSL reports. In sum, we determined that the FBI and the Department have fully implemented 23 of 28 recommendations by creating new internal controls, providing guidance and training to FBI personnel, establishing new record-keeping practices, and conducting periodic reviews of NSL usage.

Informed by the results of the compliance review described in Chapter Four, we believe that the corrective measures that have had the greatest impact on the FBI's compliance with NSL authorities are the development and consolidation of NSL policy and guidance in the Comprehensive NSL Guidance EC and later the DIOG; mandatory training provided to NSL users and approvers; the implementation of the NSL subsystem; and the periodic inspections of NSL use by the FBI Inspection Division and the NSR teams.

The NSL subsystem, in particular, reduces opportunities for human error with drop-down menus, limited choices, and self-populated fields, and ordered tasks and automated notifications ensure that each NSL receives the required legal and supervisory review and approval. At the same time,

the NSL subsystem cannot eliminate FBI errors completely as it relies upon the careful entry of accurate information. For this reason, we believe the FBI's mandatory training on NSL requirements and IOB reporting and the policies and procedures in the Comprehensive NSL Guidance EC and the DIOG deserve considerable credit for the FBI's improved compliance described in Chapter Four. Finally, periodic inspections of NSL use help ensure that NSL users and approvers remain vigilant in their attention to NSL authorities and procedures and help to identify new or reoccurring compliance issues that can form the basis for additional guidance and compliance measures.

Nevertheless, we identified areas requiring additional effort and attention by the FBI and the Department to ensure the FBI's compliance with NSL authorities. In addition to the new recommendations we make in Chapters Four and Five, we believe the FBI should take the following steps to fully implement the remaining five recommendations in our first and second NSL reports.

To further address Recommendation 3 in our second NSL report, the FBI should consider an upgrade to the NSL subsystem to require case agents to certify that the information contained in the NSL request has been checked against source documents in the case file. The FBI should also consider the efficacy of an upgrade that would require case agents to enter the target's identifying information into the subsystem twice and not accept the information when the entries do not match.

To further address Recommendations 6 in our first NSL report and 17 in our second NSL report, the FBI should provide additional information and documents establishing that the FBI has considered, and will consider in the future, the feasibility of electronic tagging as it adopts new systems that process NSL-derived information.

To further address Recommendation 2 in our second NSL report, the FBI should consider incorporating in the FBI Inspection Division's NSL reviews an examination of a sample of the data entries made in the NSL subsystem, including the entries made in connection with manually generated NSLs, to evaluate and help ensure the accuracy of the information entered into the subsystem.

Finally, to further address Recommendation 12 in our second NSL report, the FBI should consider issuing additional guidance to the field to ensure that squad supervisors understand their responsibility to verify adherence to NSL record-keeping requirements during quarterly case file reviews and revise the template for the case file review reports to have each case agent state whether all NSL-related documents are in the NSL sub-file.

PAGE INTENTIONALLY LEFT BLANK

CHAPTER THREE
REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS IN 2007 THROUGH 2009

In this chapter, we describe the FBI's use of national security letters during calendar years 2007, 2008, and 2009. In Section I, we present the FBI's data on NSL usage and discuss the trends in the data from 2007 through 2009 and from 2003 through 2009. In Section II, we describe the usefulness of NSLs as an investigative tool. We also describe a recent change in NSL use caused by the refusal, beginning in 2009, of certain Internet providers to provide electronic communication transactional records.

I. National Security Letter Requests in 2007 through 2009

In this section, we describe the FBI's use of NSLs during calendar years 2007 through 2009. Unless otherwise indicated, this report relies upon the data contained in the Department's semiannual classified reports on NSL use covering 2007 through 2009 submitted to Congress in April 2010 and March 2011. The data in the Department's semiannual classified reports was derived from two principal sources. The 2008 and 2009 NSL data was derived from the NSL subsystem. The 2007 NSL data was derived from the NSL tracking database used by the FBI OGC (OGC database) before the FBI's implementation of the NSL subsystem.

In our first and second NSL reports, we described various technical and structural problems with the OGC database used to compile the data reported in the Department's semiannual classified reports to Congress.[69] These problems resulted in inaccuracies and a significant understatement of NSL requests reported to Congress in 2003 through 2006. While noting the limitations of the OGC database, we provided a summary and analysis of the data derived in large part from that database because it was the only centralized repository of data reflecting the FBI's use of NSL authorities in 2003 through 2006.

Based on the findings in our first and second NSL reports, the FBI decided to delay further reporting of NSL data to Congress until it took steps to correct data in the OGC database. The Department ultimately submitted four comprehensive reports to Congress on April 30, 2010, one for each of the NSL statutory authorities: ECPA, RFPA, FCRAu, and FCRAv. Each

[69] NSL I Report, 31-36; NSL II Report, 104-107.

report revised the NSL data previously provided to Congress for the period of July 1, 2006, through December 31, 2006, and provided new NSL data for the period of January 1, 2007, through June 30, 2009.[70]

In these four comprehensive reports, the Department described the corrective measures the FBI had taken to improve the accuracy of the NSL data submitted to Congress, including an audit of 10 percent of the entire OGC database. The Department noted that despite the corrective measures taken, however, the FBI had reason to believe that errors continued to exist in the NSL data that pre-dated the NSL subsystem. Accordingly, while we relied upon the semiannual classified reports submitted to Congress in April 2010 as the best information available on the FBI's use of NSLs in calendar year 2007, we believe this information contains errors, the extent of which remains unknown.

The Department submitted four reports to Congress on March 28, 2011, one for each of the NSL statutory authorities for the period of July 1, 2009, through December 31, 2010. In these reports, the Department stated that the FBI relied upon the NSL subsystem to prepare the information contained in the reports and had taken steps to ensure that the small number of NSLs generated outside the subsystem (manually generated NSL) were included in the data reported.

We have greater confidence in the information submitted to Congress for calendar years 2008 and 2009. Since January 1, 2008, the FBI has relied exclusively on the NSL subsystem to compile the NSL data for congressional reporting. As case agents complete the web-based workflow to generate an NSL and approval EC, the subsystem prompts the agent to enter all the data points necessary for congressional reporting and later uses a pre-defined reporting mechanism to compile the data points and provide the statistics given to Congress. For the relatively few manually generated NSLs, case agents must send a lead that notifies the FBI OGC that a manually generated NSL has been issued and provides the FBI OGC with all the NSL data points necessary for congressional reporting.

While more reliable than the OGC database, the data compiled by the NSL subsystem may not be completely free of error. During our review, we requested spreadsheets from the FBI itemizing each NSL request issued in 2008 and 2009.[71] The itemized NSL data provided to the OIG reflect NSL

---

[70] According to the reports, the FBI had previously briefed the relevant congressional oversight committees regarding its plan to delay reporting.

[71] We requested the itemized NSL data in order to analyze the FBI's NSL usage on data points not presently captured in the Department's semiannual classified congressional reports. For example, the spreadsheets the FBI produced allowed the OIG to organize the number of NSL requests each year by investigation type (counterterrorism,

(Cont'd.)

statistics compiled by the NSL subsystem that, in the aggregate, are substantially similar but not identical to the statistics reported to Congress. Specifically, the total number of NSL requests reported to Congress in 2008 and 2009 is less than the aggregate reflected in the data provided to the OIG by 134 and 1,755 requests, respectively. The disparities are even greater comparing the data provided to Congress and the OIG on the number of requests by NSL statute – the sum of the requests reported to Congress in 2008 and 2009 is less than the sum of the requests reported to the OIG by 2,894 and 2,231, respectively.

When we requested the itemized NSL data from the FBI, we expected that the information provided would, in the aggregate, mirror the data provided to Congress, particularly since the data provided to the OIG and to Congress both came from the NSL subsystem. The FBI Unit Chief who manages the FISA Management System, which includes the NSL subsystem, told us that the numbers do not match because although the data provided to Congress and the OIG came from the NSL subsystem, the manner in which the NSL subsystem gathered the data was different. She told us that the NSL subsystem uses a pre-defined reporting mechanism, which she described as a "front-end" reporting mechanism, to generate aggregate numbers on the data points required by Congress. She said that the spreadsheets containing the additional information requested by the OIG required the use of a search tool that retrieved the NSL data from the "back-end" of the subsystem.

Whether NSL data is retrieved using a pre-defined reporting mechanism or a search tool, we would generally expect the statistics on the same data points to be identical, or almost identical given that there could be a slight variation caused by a time lag in the "expression" of manually generated NSL data into the subsystem.[72] The disparities we found,

---

counterintelligence, and cyber intrusion investigations) and by NSL type (telephone toll records, telephone subscriber only, electronic communication transactional records, electronic subscriber only, financial records, full credit reports, and financial institution and consumer-identifying information under FCRAu(a) and (b)), as illustrated later in this chapter.

[72] After the FBI OGC receives a lead from the field that notifies the FBI OGC's NSLB of a manually generated NSL, the NSLB's FISA Unit enters the data points for the NSL that are necessary for congressional reporting into the NSL subsystem. The FISA Unit refers to this process as the "expression" of manually generated NSLs into the NSL subsystem. If two reports having the same parameters are generated by the NSL subsystem at different times and one report is generated before and the other is generated after certain manually generated NSLs falling within the reports' parameters are expressed into the NSL subsystem, the reports would not produce identical results. We would expect the difference, however, to be nominal given the relatively small number of manually generated NSLs issued by the FBI. For example, as described in the next chapter, the FBI's Inspection Division found during its 2009 internal review of NSLs that the FBI issued [redacted] (Cont'd.)

however, are more than nominal and therefore would not seem to be explained by the relatively small number of manually generated NSLs issued during the period of our review.[73]

Without an audit of the NSL subsystem itself, it is not possible to determine whether the disparities we identified reflect errors or anomalies in the data reported to Congress or in the data reported to the OIG, or possibly both. At a minimum, the disparities suggest that data compiled through the use of the NSL subsystem may not be free of error.[74]

Further, we found internal irregularities or inconsistencies in the itemized data provided to us by the FBI. We identified 1,232 records in the spreadsheets that provided no NSL data other than the NSL identification number and basic case information (case number, investigative subject, and U.S. person status). The records do not reflect the number of NSL letters or requests associated with the NSL identification number or a breakdown of the number of requests and letters by NSL statute and NSL type. In addition, we identified seven records in which the total number of letters noted in the spreadsheet does not match the aggregate number of letters broken down by NSL type.

One final caveat before describing the FBI's statistics on NSL usage in 2007 through 2009 is that, unrelated to how the NSL subsystem compiles data, the NSL data reported to Congress and to the OIG does not include all of the manually generated NSLs that were issued by the FBI in 2008 and 2009. Because the FBI's process for notifying the FBI OGC about the issuance of manually generated NSLs is not automated, there can be no guarantee that all of the manually generated NSLs were reported to the FBI

---

manually generated NSLs between December 1, 2008 and December 1, 2009, as compared to a total of 30,442 NSL requests issued between January 1, 2009, and December 31, 2009.

[73] After reviewing the draft of this report, the FBI told the OIG for the first time that the NSL data provided to Congress would almost never match the NSL data provided to the OIG because the NSL data provided to Congress includes NSLs issued from case files marked "sensitive," whereas the NSL data provided to the OIG does not. According to the FBI, the unit that provided NSL data to the OIG does not have access to case files marked "sensitive" and was therefore unable to provide complete NSL data to the OIG. The assertion that the FBI provided more NSL data to Congress than to the OIG does not explain the disparities we found in this review, however, because the disparities we found reflected that the FBI reported fewer NSL requests to Congress than the aggregate totals provided to the OIG.

[74] After reviewing the draft of this report, the FBI told the OIG that while 100 percent accuracy can be a helpful goal, attempting to obtain 100 percent accuracy in the NSL subsystem would create an undue administrative burden without providing corresponding benefits. The FBI also stated that it has taken steps to minimize error to the greatest extent possible.

OGC for inclusion in the Department's semiannual classified congressional reports. Indeed, as described in the next chapter, the FBI's Inspection Division found during its internal review of NSLs issued by the FBI in calendar year 2009 that the field failed to report to the FBI OGC [redacted] percent, or [redacted] out of [redacted], of the manually generated NSLs issued in 2009 and that the FBI did not have an adequate mechanism for tracking manually generated NSLs. While this finding indicates that the field failed to report a significant percentage of manually generated NSLs to the FBI OGC in 2009, the total number of manually generated NSLs that the FBI inspectors identified is relatively small compared to the total number of 30,442 NSL requests issued by the FBI that year. What remains unknown, however, is whether the FBI inspectors identified all of the manually generated NSLs issued by the FBI or whether a significant number remains unaccounted for and unreported.

With these caveats, we discuss below the data provided by the FBI on its NSL usage for calendar years 2007 through 2009.

A. Methodology

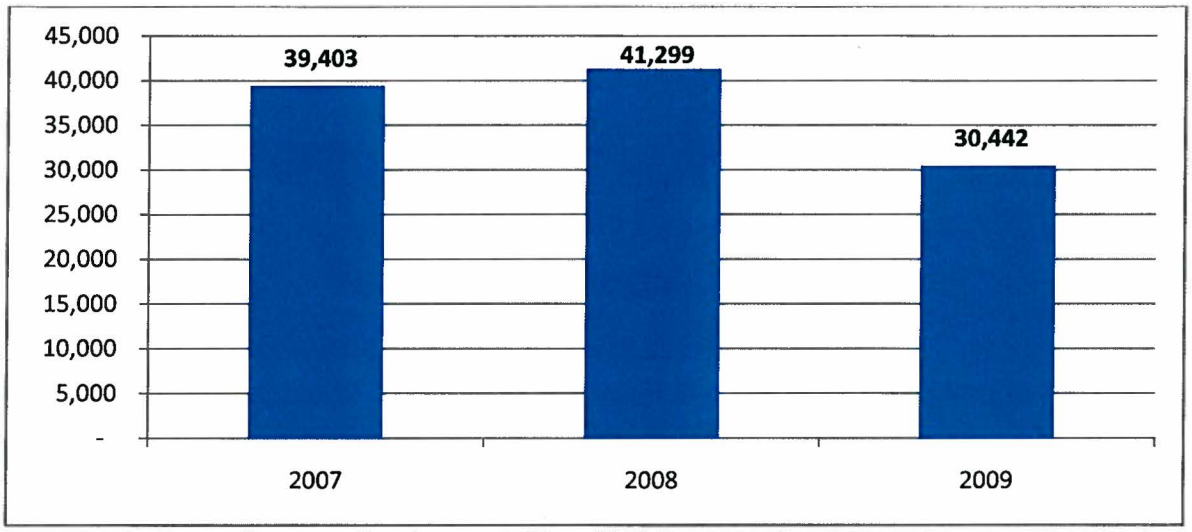
We examined the NSLs and NSL requests issued during the three types of investigations in which NSLs are authorized: counterterrorism, counterintelligence, and foreign computer intrusion cyber investigations. Except as otherwise noted, we describe the number of NSL requests rather than the number of national security letters because one letter may include more than one request. Further, the data presented in the Department's semiannual classified reports to Congress and in its annual public reports describe the numbers of requests made, not the number of letters issued. In this report, we follow that same approach unless otherwise noted.

B. Description of National Security Letter Requests in 2007 through 2009

In this section, we describe the total number of NSL requests issued by the FBI in 2007, 2008, and 2009. We also categorize the total number of NSL requests in each year by statutory authority invoked, type of records requested, type of investigation (counterterrorism, counterintelligence, and cyber intrusion), and U.S. person status of the investigative subject.

Figure 3.1 depicts the total number of NSL requests issued by the FBI in each year.

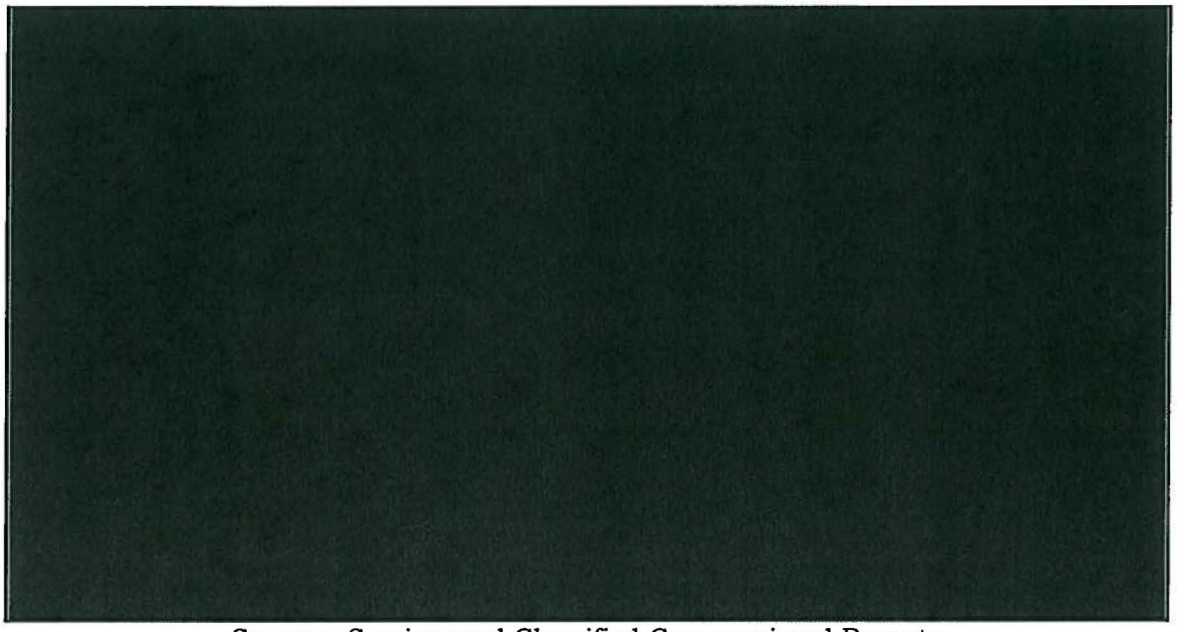
FIGURE 3.1: NSL Requests 2007-2009



Source: Semiannual Classified Congressional Reports

As shown in Figure 3.2 below, the vast majority of NSL requests issued by the FBI in 2007 through 2009 sought telephone and electronic records under the ECPA.

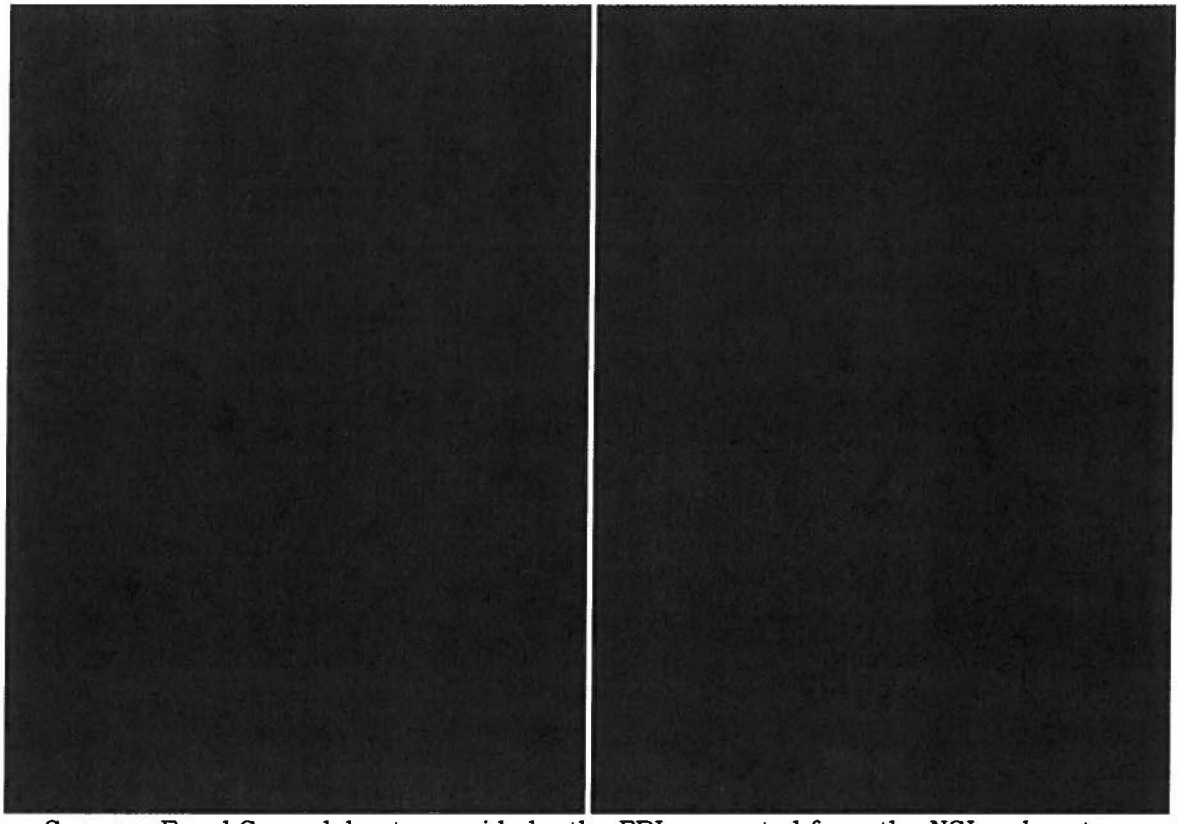
FIGURE 3.2: NSL Requests by Statutory Authority 2007-2009



Source: Semiannual Classified Congressional Reports

As shown in Figure 3.3, the FBI issued a majority of its NSL requests in furtherance of counterterrorism investigations and a significant number of NSL requests in counterintelligence investigations. The FBI issued substantially fewer requests in furtherance of cyber intrusion investigations.

FIGURE 3.3
NSL Requests in Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations 2008-2009[75]



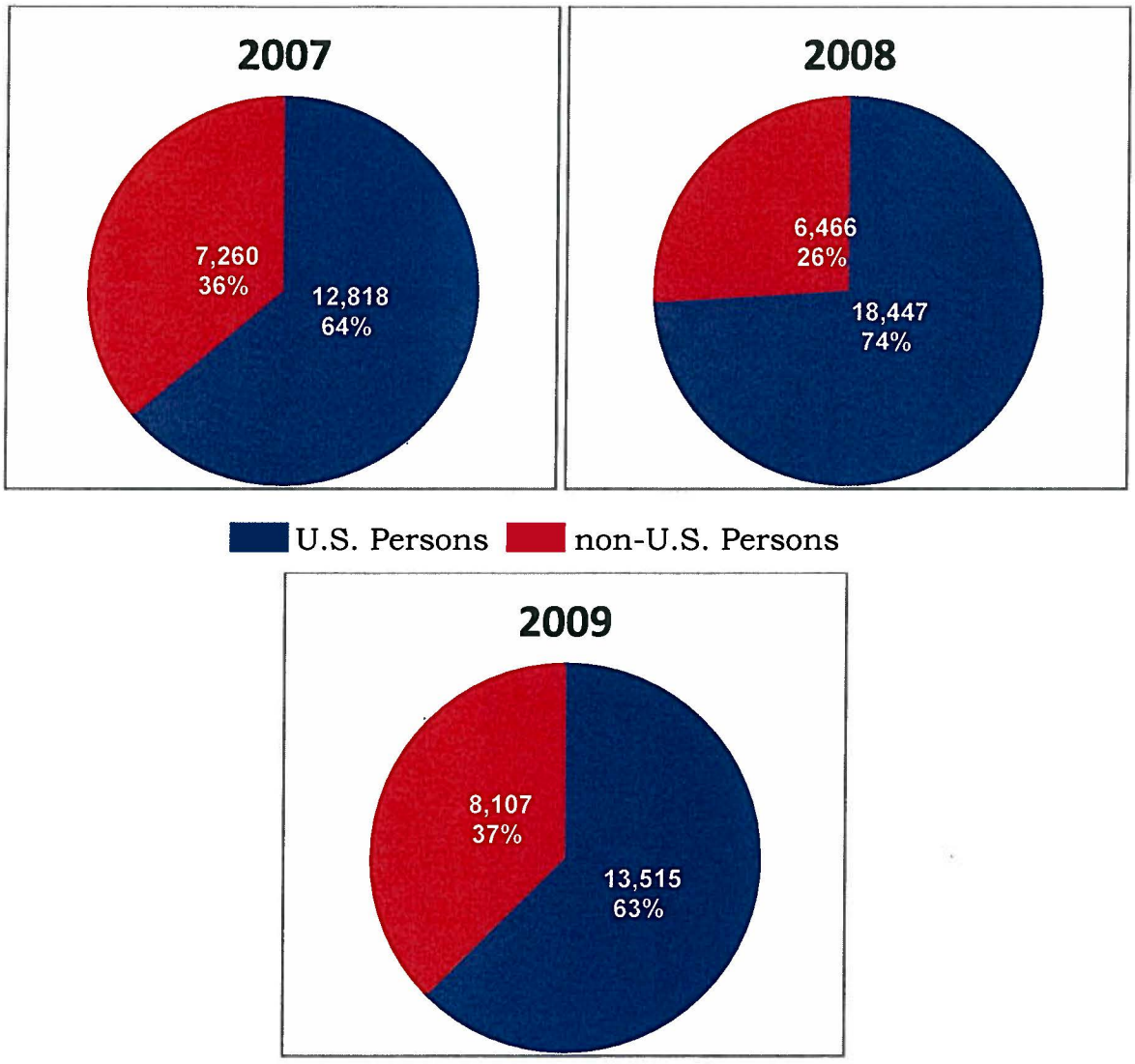
Source: Excel Spreadsheets provide by the FBI generated from the NSL subsystem

Counterterrorism Counterintelligence Cyber

[75] The source of this information is the NSL data the FBI produced to the OIG in itemized spreadsheets. The semiannual classified congressional reports do not provide NSL statistics by investigation type. As described above, the NSL data in the itemized spreadsheets does not exactly match the NSL data reported to Congress in 2008 and 2009. The total number of NSL requests in Figure 3.3 for each year is more than the total number of NSL requests reported to Congress by 134 and 1,755 requests, respectively. In addition, this chart excludes NSLs issued in 2007 because the FBI did not provide the OIG with relevant data for 2007. FBI officials told us that the only data source for 2007 other than the semiannual classified reports is the OGC database and that the database is retired and unavailable.

As shown in Figure 3.4, the FBI issued the majority of NSL requests in 2007 through 2009 in furtherance of investigations of U.S. persons.

FIGURE 3.4: NSL Requests Relating to Investigations of U.S. Persons and Non-U.S. Persons 2007-2009[76]

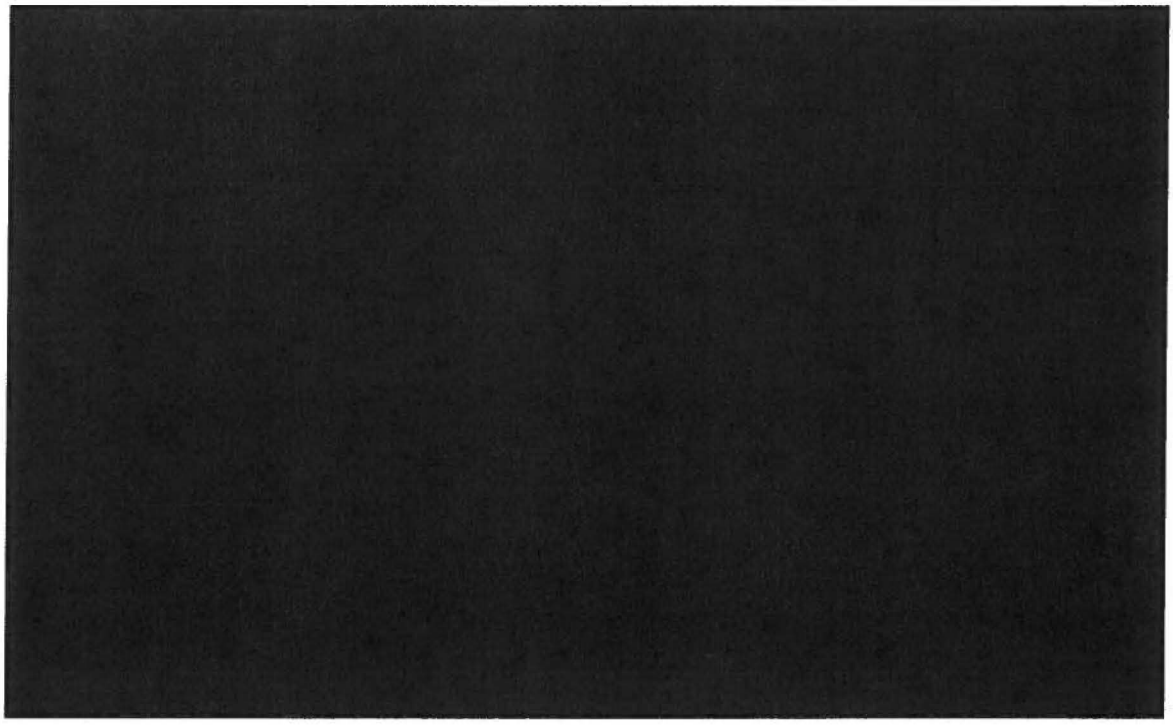


Source: Semiannual Classified Congressional Reports

[76] The information reflected in these charts does not include information on the U.S. person status relevant to subscriber-only NSL requests under ECPA, which the Department did not report to Congress. According to the FBI, when the FBI issues an NSL for "subscriber only" information, the FBI generally does not have, and may never obtain, information as to the person's U.S. person status. For this reason, the FBI did not report the U.S. person status associated with subscriber-only NSLs.

As shown in Figures 3.5 and 3.6, NSL requests for telephone subscriber information comprised the largest percentage of NSL requests in 2008, followed by requests for telephone toll records and financial records. In 2009, telephone toll records comprised the largest percentage, followed by telephone subscriber information and electronic communication transactional records.[77]

FIGURE 3.5: 2008 NSL Requests by NSL Type

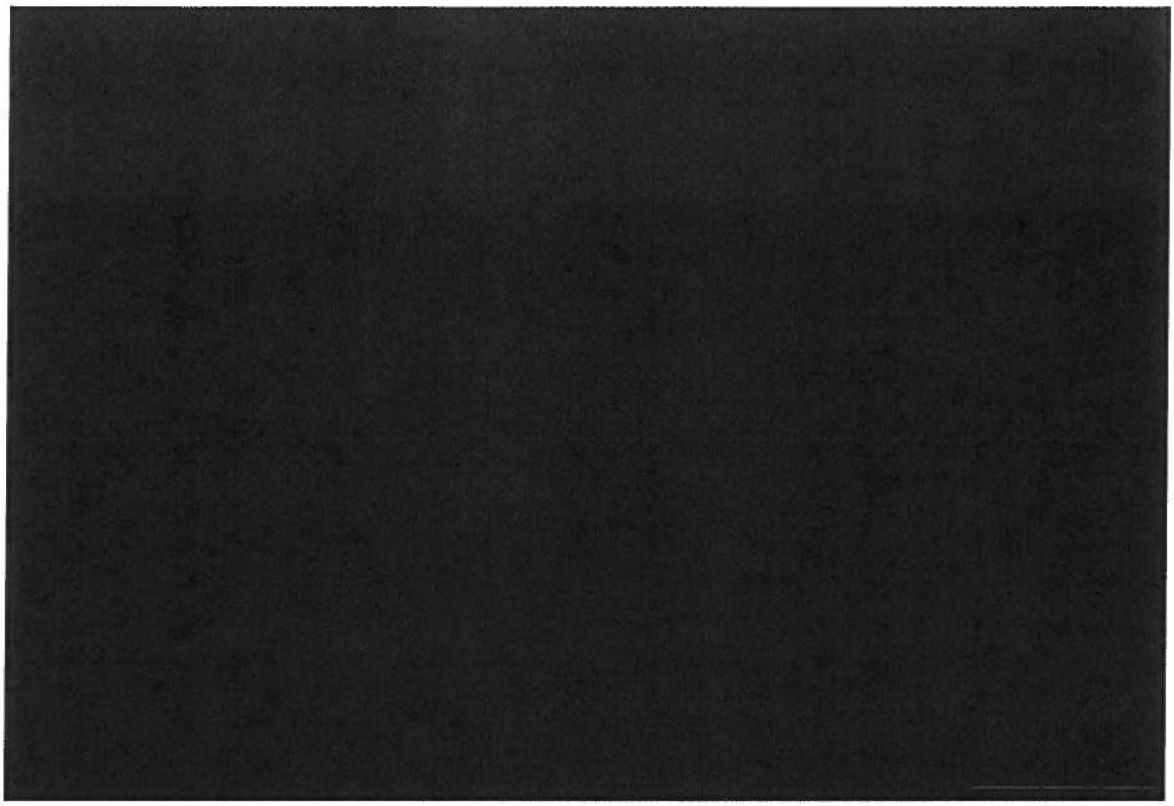


TTR = Toll Billing Records	FR = Financial Records
TSI = Telephone Subscriber Information	FIL = Financial Institution Listings
ECTR = Electronic Communication Transactional Records	CII = Consumer Identifying Information
ESI = Electronic Subscriber Information	FCR = Full Credit Reports

Source: Excel Spreadsheets provide by the FBI generated from the NSL subsystem

[77] The source of this information is the NSL data the FBI produced to the OIG in itemized spreadsheets. The semiannual classified congressional reports do not provide NSL statistics by investigation type. As described above, the NSL data in the itemized spreadsheets does not exactly match the NSL data reported to Congress in 2008 and 2009. The total number of requests in Figures 3.5 and 3.6 for each year is more than the total number of NSL requests reported to Congress by 2,894 and 2,231 requests, respectively. In addition, this chart excludes NSLs issued in 2007 because the FBI did not provide the OIG with relevant data for 2007. FBI officials told us that the only data source for 2007 other than the semiannual classified reports is the OGC database and that the database is retired and unavailable.

FIGURE 3.6: 2009 NSL Requests by NSL Type



TTR = Toll Billing Records	FR = Financial Records
TSI = Telephone Subscriber Information	FIL = Financial Institution Listings
ECTR = Electronic Communication Transactional Records	CII = Consumer Identifying Information
ESI = Electronic Subscriber Information	FCR = Full Credit Reports

Source: Excel Spreadsheets provide by the FBI generated from the NSL subsystem

C. Trends in National Security Letter Usage from 2003 through 2009

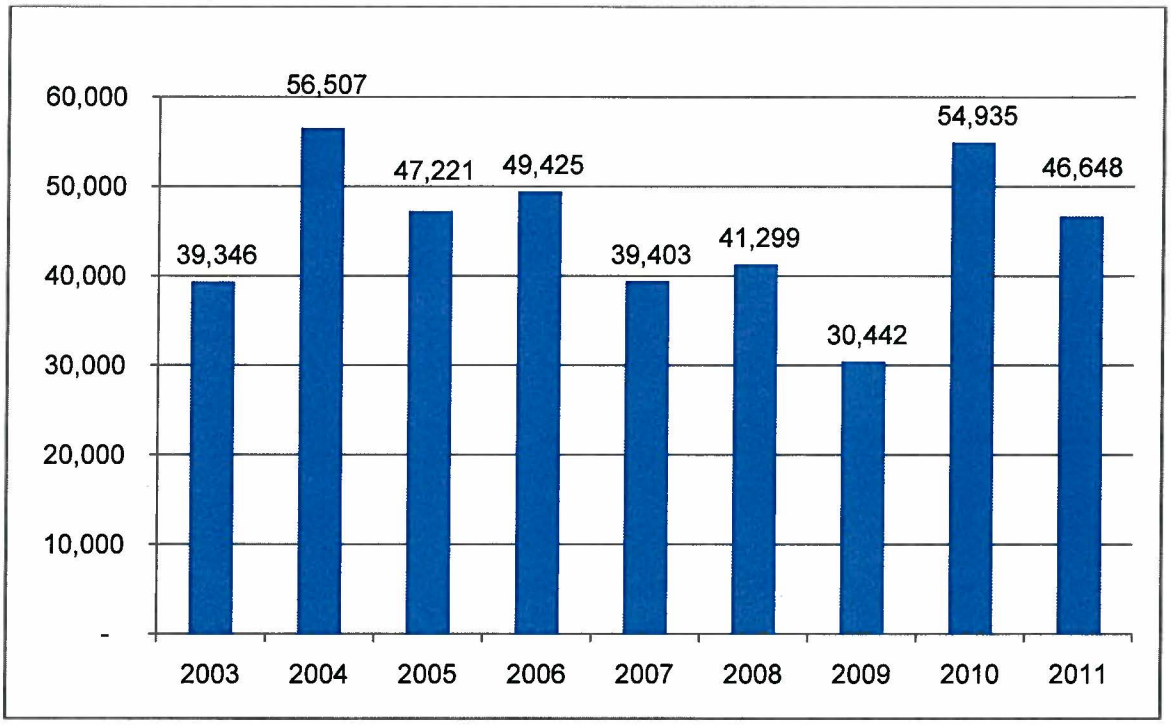
In this section, we describe the trends in the FBI's NSL requests from 2003 through 2009 as documented in the Department's semiannual classified reports to Congress, our review of the OGC database in our first and second NSL reviews, and in the NSL data provided to the OIG in this review, when applicable.

According to the Department's semiannual classified reports to Congress covering 2007 through 2009, the FBI issued a total of 111,144 NSL requests during 2007 through 2009. The individual totals for 2007, 2008, and 2009 varied as shown in Figure 3.1, and the average annual number of requests for the period was approximately 37,048. By comparison, the FBI issued approximately 51,051 NSLs per year between

2004 and 2006, and approximately 48,125 NSL requests per year between 2003 and 2006.[78] Thus, the FBI issued significantly fewer NSL requests during 2007 through 2009 than during 2003 through 2006.

The Department's most recent semiannual classified reports to Congress, however, indicate that the FBI's NSL use returned to historically typical numbers after 2009 – 54,935 NSL requests in 2010 and 46,648 in 2011.[79]

FIGURE 3.7: NSL Requests 2003-2011



Source: Semiannual Classified Congressional Reports

[78] In our second NSL report, we reported that the FBI issued a total of 192,499 NSL requests during 2003 through 2006. This number consisted of [redacted] requests reported to Congress in the Department's original semiannual classified reports covering 2003 through 2006 and [redacted] NSL requests for consumer full credit reports issued from 2003 through 2005 that the Department was not required to report to Congress. NSL II Report, at 109; NSL I Report, 36.

[79] *See* the Department's semiannual classified reports submitted to Congress on March 28, 2011 covering July 1, 2009, through December 31, 2010, the reports submitted on December 29, 2011, covering January 1, 2011, through June 30, 2011, and the reports submitted on February 8, 2012, for the semiannual periods covering July 1, 2011, through December 31, 2011.

The factors that may have contributed to the decrease in NSL usage from 2007 through 2009 as compared to previous years are not evident from the data we reviewed. Although the OIG requested an explanation from the FBI for the decrease in NSL usage during this period, the FBI represented that neither the Department nor the FBI had a process in place to identify the reasons for the change in NSL usage from year to year. According to the FBI, the number of NSLs issued in any given year is a function of the needs of the national security investigations conducted during that year.

During our field visits, we asked FBI personnel whether they had observed any changes in the FBI's or their own use of NSLs in the last five years. Most field personnel we interviewed told us that they had not observed any changes in NSL use. However, two supervisors and a division counsel told us that they believe agents use NSLs less often now than they did five years ago. These individuals told us that because of increased scrutiny on NSL use agents employ alternative investigative tools when possible. We have no information that these observations are representative of the experience in the field generally, and we note that the NSL data for 2010 and 2011 shown in Figure 3.7 does not indicate a continued trend of less frequent NSL use by the FBI.

Similarly, the data does not reveal the factors that contributed to the FBI issuing only 30,442 NSL requests in 2009, the lowest number of annual requests during the 9-year period depicted in Figure 3.7. Further, available information from the Department's semiannual classified reports indicates that during 2009, the FBI issued substantially fewer subscriber-only NSLs pursuant to the ECPA – only [redacted] as compared to [redacted] in 2008 and [redacted] in 2007. Steven Siegel, the former Deputy General Counsel of the FBI OGC's National Security Law Branch between September 2009 and April 2012, told us that 2009 was an "anomaly" from a statistical perspective and that the FBI would need to devote a substantial amount of resources to determine the reasons for the significant decrease in NSL use that year, an effort that the FBI has not undertaken.

Finally, the NSL data reflected in Figure 3.4 shows that well more than half of the FBI's NSL requests in 2007 through 2009 were generated from investigations of U.S. persons: 12,818, or 64 percent, in 2007; 18,447, or 74 percent, in 2008; and 13,515, or 63 percent, in 2009. This data indicates that the shift reported in our second NSL review toward more NSL requests generated from investigations of U.S. persons as compared to non-U.S. persons – from 39 percent in 2003 to 57 percent in 2006 – continued in 2007 through 2009.[80]

---

[80] NSL II Report, 110-112.

II. Usefulness of National Security Letters as an Investigative Tool

A. National Security Letters as an Investigative Tool

In our first and second NSL reports, we examined the effectiveness of national security letters as an investigative tool in national security investigations conducted between 2003 and 2006.[81] In our first NSL report, we described the principal uses of NSLs and the value of each NSL type to an investigation. We described how the FBI uses NSLs to develop evidence to support applications for Foreign Intelligence Surveillance Act (FISA) 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 (JTTF), 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.

We also reported that the FBI uses information derived from NSLs (and other investigative tools) to generate a variety of analytical intelligence products, 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 JTTFs, and disseminated to other federal agencies and the intelligence community. The FBI also provides information derived from NSLs to law enforcement authorities for use in criminal proceedings.[82]

In our second NSL report, we reported that the FBI continued to find the NSL to be an important investigative tool in national security investigations conducted in 2006. To illustrate, we provided examples of the value of NSLs issued in specific investigations.

In this review, our interviews of FBI Headquarters officials and field personnel, as well as our examination of case files and the FBI's data on

---

[81] NSL I Report, 45-65; NSL II Report, 114-116.

[82] After reviewing a draft of this report, the FBI stated that it provides NSL-derived information to law enforcement authorities on "rare occasions." As we noted in our first NSL review, it is difficult to determine how often the FBI provides NSL-derived information to law enforcement authorities for use in criminal proceedings 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. NSL I Report, 62-63.

NSL usage, showed that the national security letter continued to be an important tool in the FBI's national security investigations conducted in 2007 through 2009. Most FBI personnel told us that the national security letter is an important intelligence tool, using adjectives such as "crucial," "vital," and "indispensible" to describe its continued value.

We found that the FBI used NSLs in 2007 through 2009 in the same ways it had used NSLs in previous years. Almost all field personnel we interviewed told us that they used NSLs to identify an investigative [redacted].

To identify a [redacted], field personnel most often issued NSL requests pursuant to ECPA for telephone toll billing records and electronic communication transactional records. Field personnel told us that in instances where they have been uncertain as to whether [redacted] subject or other person of interest to an investigation, they have issued ECPA NSL requests for telephone or electronic subscriber information only (which is limited to name, address, and length of service), [redacted] on the account before issuing a [redacted]. Field personnel told us that they have also used subscriber-only NSL requests to [redacted].

Field personnel told us that they issued NSL requests pursuant to RFPA for financial records to determine whether [redacted]. Case agents told us that they have also used financial records to identify [redacted] because these records can show financial [redacted]. In instances where the [redacted].

We found that FBI personnel in the field divisions we visited used NSLs at various stages in the investigation – near the beginning, towards the end, or at any time throughout in response to new information gathered during an investigation. Field personnel told us that they have used NSLs near the beginning of a preliminary or full investigation after checking open sources and before employing more intrusive techniques. The use of NSLs during these early investigative steps can provide information that helps the FBI determine whether or not to pursue an investigation further. NSLs can

also be issued at the end of an investigation to confirm that case closure is appropriate.

To further assess the usefulness of NSLs in national security investigations, we asked several FBI personnel in the two field divisions we visited to identify alternative investigative techniques to the NSL. We also asked them to describe the effectiveness of these alternative tools in determining whether an investigative subject is associated with known terrorists or terrorist organizations or subjects in other investigations and whether an investigative subject has suspicious financial activity or is financially susceptible to recruitment or exploitation. As described below, FBI personnel told us that alternative tools to obtain the same information either do not exist or are less effective.

FBI personnel told us that in cases that have a criminal nexus the FBI can use a grand jury subpoena to obtain information that is substantially similar to the information obtained through an NSL. [redacted].

FBI personnel identified other alternatives for determining [redacted]. They told us that these alternatives were less effective than NSLs because the techniques require more resources and can produce information that is not as complete or reliable as NSL-derived information. They also stated that these techniques create a greater risk of premature exposure of the investigation. Two FBI employees also said that [redacted] may unnecessarily intrude on a potentially innocent person's privacy and can harm his or her reputation in the community.

We interviewed two field supervisors on cyberterrorism squads who told us that in cyber intrusion investigations there is often no alternative to an NSL because the only lead in the case is [redacted]. In those instances, [redacted] can only be accomplished with [redacted].

A few case agents described one disadvantage of using the NSL as an investigative tool. These agents told us that they experienced significant delays in receiving NSL return data from certain providers. The agents said that they have had experiences where they waited months for providers to produce the requested information and that such delays can hamper an investigation.

Finally, we asked several FBI personnel whether they had observed any changes in the use or usefulness of NSLs in last 5 years. While most FBI personnel told us that they have observed no significant changes in how NSLs are used, a few described the refusal of certain Internet providers beginning in 2009 to provide electronic communication transactional records in response to NSLs. Because this refusal has had a significant impact on NSL usage and effectiveness, we describe the issue in more detail below.

B. National Security Letter Requests for Electronic Communication Transactional Records

The FBI has historically interpreted Section 2709 of ECPA as granting the FBI the authority to compel wire and electronic communication service providers to provide electronic communication transactional records, and it has routinely sought and obtained such records through ECPA NSLs. In a change from its past practice, in 2009, [redacted], refused to provide transactional records to the FBI in response to ECPA NSLs on the ground that Section 2709 does not grant the FBI the authority to compel the production of electronic communication transactional records. [redacted] eventually followed suit.[83]

The relevant statutory language in Section 2709 states:

> **(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:

---

[83] According to an Assistant General Counsel in the FBI OGC's NSLB, [redacted] had refused to provide certain [redacted] sometime before they refused to provide transactional records altogether. Recollections varied during our interviews with FBI personnel about exactly when [redacted] first communicated its intention to no longer produce any electronic communication transactional records to the FBI in response to NSLs. Based upon our review of ECPA NSLs issued by the Boston and San Francisco field divisions, it appears that [redacted] stopped producing transactional records by November 2009 at the latest.

> **(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.

Thus, the term "electronic communication transactional records" appears in Section 2709(a)'s description of the types of record requests wire and electronic communication service providers must comply with under Section 2709(b), but these records are not included in Section 2709(b)'s list of records that the FBI may obtain under this authority.

As originally enacted in 1986, subsection (a) provided the only list of records subject to NSL authority under Section 2709 – subscriber information and toll billing records information, or electronic communication transactional records – and subsection (b) merely stated that the FBI could request such records with the appropriate written certification. *See* Pub. L. No. 99-508 § 201. In 1993, when Congress added to subsection (b) the specification of "name, address, length of service, and toll billing records," without explanation in the legislative history it did not include "electronic communication transactional records" in that list. *See* Pub. L. No. 103-142.

The decision of these [redacted] Internet companies to discontinue producing electronic communication transactional records in response to NSLs followed public release of a legal opinion issued by the Department's Office of Legal Counsel (OLC) regarding the application of ECPA Section 2709 to various types of information. The FBI's General Counsel sought guidance from the OLC on, among other things, whether the four types of

information listed in subsection (b) of Section 2709 – the subscriber's name, address, length of service, and local and long distance toll billing records – are exhaustive or merely illustrative of the information that the FBI may request in an NSL. In a November 2008 opinion, the OLC concluded that the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL.

Although the OLC opinion did not focus on electronic communication transactional records specifically, according to the FBI, [redacted] took a legal position based on the opinion that if the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL, then the FBI does not have the authority to compel the production of electronic communication transactional records because that term does not appear in subsection (b).

The FBI OGC disagrees with this legal position, relying, in part, upon a discussion contained in a footnote in the OLC opinion that addressed the incongruity between Sections 2709(a) and (b). The OLC stated that its conclusion that subsection (b) is exclusive is not undermined by the fact that the term "electronic communication transactional records" appears in subsection (a) only. Relying upon the legislative history from 1986 ("electronic communication transactional records" in subsection (a) gives the FBI "the necessary authority [to issue NSLs] with regard to subscriber information and toll billing information with respect to electronic communication services other than ordinary telephone service"), the OLC stated:

> While [the legislative history clarifies] that NSLs can extend to other types of services, the [statutory] language reaches only those categories of information parallel to subscriber information and toll billing records for ordinary telephone service.

Drawing support from this footnote, the FBI OGC has maintained that the FBI has the authority under Section 2709 to obtain electronic communication transactional records because those records parallel toll billing records.[84]

The resolution of this issue has significant consequences for the FBI's use of NSLs. Steven Siegel told us that [redacted] percent of the NSLs issued

---

[84] Supervisors in the Operations Section of the Department's National Security Division told us that the FBI presented this legal issue to the NSD in early 2010. According to these supervisors, the NSD considered the issue and, after informally consulting with representatives of the OLC, ultimately agreed to support the FBI's view of the statute.

by the FBI for electronic communication transactional records are directed to [redacted].

To address what has become an impasse between the FBI and the Internet companies, the Department has considered proposing legislation that would clarify the FBI's ability to request and obtain electronic communication transaction records under Section 2709(b).

In the absence of a legislative amendment to Section 2709, [redacted].[85] Siegel told us that the process of generating and approving a Section 215 application is similar to the NSL process for the agents and supervisors in the field, but then the applications undergo a review process in NSLB and the Department's National Security Division, which submits the application to the Foreign Intelligence Surveillance Court (FISA Court). According to Siegel, a request that at one time could be accomplished with an NSL in a matter of hours if necessary, now takes about 30-40 days to accomplish with a standard Section 215 application.[86]

In addition to increasing the time it takes to obtain transactional records, Section 215 requests, unlike NSL requests, require the involvement of FBI Headquarters, NSD, and the FISA Court. Supervisors in the Operations Section of NSD, which submits Section 215 applications to the FISA Court, told us that the majority of Section 215 applications submitted to the FISA Court [redacted] in 2010 and [redacted] in 2011 – concerned requests for electronic communication transactional records.[87]

The NSD supervisors told us that at first they intended the [redacted]. They told us that when a legislative change no longer appeared imminent, and [redacted]

---

[85] [redacted].

[86] According to the NSD, the FBI can formally request that the NSD expedite the preparation of any FISA application when necessary.

[87] [redacted]

[redacted] and by taking steps to better streamline the application process.

We asked whether the disagreement and uncertainty over electronic communication transactional records has negatively affected national security investigations. An Assistant General Counsel in NSLB told us that the additional time it takes to obtain transactional records through a Section 215 application slows down national security investigations, all of which he said are time-sensitive. He said that an investigative subject can cease activities or move out of the country within the time-frame now necessary to obtain a FISA order.

Based upon the foregoing, we believe the Department should continue its efforts to bring about a legislative amendment to Section 2709 that will provide greater clarity to the issue of whether electronic communication transactional records can be requested and obtained through an ECPA NSL.

CHAPTER FOUR
OIG FINDINGS ON THE FBI'S COMPLIANCE WITH NSL REQUIREMENTS IN 2008 AND 2009

In this chapter, we describe our findings regarding the FBI's compliance with NSL requirements set forth in the NSL statutes, Attorney General Guidelines, and the FBI's internal policies.[88]

We focused the compliance portion of our review on NSLs issued between January 1, 2008, and December 31, 2009, after the FBI implemented the NSL subsystem in all field divisions. As described in Chapter Two, the NSL subsystem significantly changed how the FBI generates NSLs, and created a mechanism for tracking the status and scope of NSL return data. We therefore concluded that examining NSLs issued before the subsystem became mandatory on January 1, 2008, would be less instructive to our assessment of the FBI's progress in implementing our recommendations than would examining NSLs issued after that date. In addition, because 2007 was a transitional year in terms of the FBI's implementation of corrective measures, we believe that the previous reviews of the FBI's use of NSLs in 2003 through 2005 and in 2006 provide a more accurate benchmark upon which to measure any progress the FBI has made since implementing the NSL subsystem.

To conduct this portion of our review, we analyzed the potential IOB violations that FBI personnel self-reported to the FBI OGC in 2008 and 2009 arising from the FBI's use of NSLs. We also examined the findings of numerous internal compliance reviews that the FBI and the Department's National Security Division conducted during the same time period as a result of our previous NSL reviews. As described later in this chapter, those reviews generally showed that the FBI achieved greater compliance with NSL requirements as a result of the corrective measures taken by the FBI and the Department in response to our first and second NSL reviews. Finally, we examined a judgmental sample of NSLs in two FBI field offices as an additional measure of the FBI's compliance.

In Section I of this chapter, we describe the NSL-related potential IOB violations reported to the FBI OGC by FBI personnel in 2008 and 2009. In Section II, we describe and analyze the findings made by the FBI's Inspection Division in its internal compliance reviews of NSLs in 2008 and

---

[88] "Attorney General Guidelines" refers to the 2003 Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), which were in effect from October 2003 to December 2008, and the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), which took effect in December 2008.

2009 and those made by the Department in its National Security Reviews. In Section III, we describe our findings based upon our examination of a judgmental sample of NSLs issued in 2008 and 2009. In Section IV, we provide our conclusions and recommendations.

As we describe in the sections that follow, our compliance review revealed that the corrective measures taken by the FBI and the Department in response to the findings and recommendations made in the OIG's first and second NSL reports had a meaningful impact on the FBI's use of NSLs in 2008 and 2009. Although we identify ongoing compliance challenges in certain areas, we found that the corrective measures that have been taken since our prior reviews generally resulted in substantial improvement in the FBI's compliance with NSL requirements.

I. Potential IOB Violations Reported to FBI OGC Arising From National Security Letters

The most serious NSL-related compliance failures are those that result in potential intelligence violations that must be reported to the Intelligence Oversight Board (IOB). In this section, we describe the relevant IOB reporting criteria and procedures and analyze the NSL-related potential IOB violations reported to the FBI OGC by FBI personnel in 2008 and 2009.

A. IOB Reporting Criteria

Executive Order 13462, signed by the President on February 29, 2008, and amended by Executive Order 13516 on October 28, 2009, directs that any intelligence activities that may be unlawful or contrary to an executive order or presidential directive be reported to the IOB and the Director of National Intelligence (DNI).

On July 17, 2008, the IOB and DNI jointly issued criteria for reporting such matters and instructions on the timing and content of the reports. The criteria require the reporting of any intelligence activity for which there is reason to believe the activity may be unlawful or contrary to executive order or presidential directive. The criteria also provide that reporting may include violations of procedures or guidelines that have potential presidential interest or involve an apparent violation of the substantive rights of individuals. Matters deemed "significant or highly sensitive," whether or not unlawful or contrary to Executive Order or Directive, must

be reported immediately.[89] Other reportable matters must be reported on a quarterly basis.

To comply with Executive Order 13462 and the related reporting criteria, the FBI developed internal procedures for reporting potential intelligence violations to the FBI OGC. These procedures are set forth in a policy guide issued on April 22, 2009, entitled, "Guidance on Intelligence Oversight Board (IOB) Matters, Policy Implementation Guide" (IOB policy). Relevant to this review, the IOB policy provides that violations of the NSL statutes must be reported to the FBI OGC as a potential IOB matter. Significant or highly sensitive matters must be reported to the FBI OGC immediately and all other matters within 30 days of discovery.[90]

The IOB policy includes the following specific examples of NSL-related intelligence violations:

- serving an NSL that contained a substantive typographical error, such as an incorrect telephone number or target name, even if the provider did not respond to the request;
- serving an NSL that requested information that is beyond the scope allowed by the applicable statute (such as requesting content information in an NSL for telephone or e-mail transactional records or a full credit report in a counterintelligence investigation);
- serving an NSL in the absence of an open predicated investigation;
- serving an NSL that sought information that was not relevant to an authorized investigation;
- serving an NSL when the investigative file lacked predication or sufficient justification to support the issuance of an NSL;
- serving an NSL that lacked approval of an authorized Senior Executive Service official; and
- receiving information that is beyond the scope permitted by statute or beyond the scope requested in the NSL and using the information or uploading the information into an FBI database.

---

[89] Under the July 17, 2008, reporting criteria, "significant or highly sensitive matters" are developments or circumstances involving intelligence activities that could impugn the reputation or integrity of the Intelligence Community or otherwise call into question the propriety of intelligence activities.

[90] In our second NSL report, we described the FBI's previous internal procedures and guidance issued in November 2006 regarding the identification and reporting potential IOB violations. NSL II Report, 135-137.

The IOB policy, which applies to all matters reported on or after April 22, 2009, regardless of whether they occurred before that date, superseded the previous guidance memoranda issued by the FBI OGC that we described in our first and second NSL reports.

The most significant difference between the current IOB policy and previous FBI OGC guidance regarding NSLs is that the current IOB policy clarified that case agents are no longer required to report as a potential intelligence violation to the FBI OGC an unauthorized collection caused by a third party error unless the third party error was compounded by the FBI's use or uploading of unauthorized information.[91] If the FBI did not compound the error in such a manner, case agents must notify the FBI OGC of such incidents within 90 days of discovery for tracking purposes only. Previous instructions required that case agents report all third party errors as potential intelligence violations regardless of whether the FBI compounded the third party error through the use or uploading of unauthorized information.

The FBI OGC made this policy change [redacted], that the FBI need not require the reporting of uncompounded third party errors to the FBI OGC as potential IOB matters.[92] Accordingly, in our review of a judgmental sample of NSLs

---

[91] As we described in Chapter Two, this report uses the term "unauthorized information" to describe information the FBI obtained from a third party provider that the provider was prohibited by statute to disclose to the FBI. This report uses the term "overcollection" to describe information obtained from a third party provider that is beyond the scope of an NSL request and the term "unauthorized collection" to describe overcollections that contain unauthorized information. Documents produced to the OIG in this review show that the FBI and the Department have most often used the term "overproduction" to describe overcollections and unauthorized collections. For consistency and clarity, in this report we use the terms "overcollection" and "unauthorized collection" rather than "overproduction."

[92] As we described in our second NSL report, on August 1, 2007, [redacted] FBI OGC to report to the IOB all third party errors that the FBI compounded through the FBI's use of the "inappropriately provided information" or the uploading of the information into an FBI database. NSL II Report, 99-100 n. 81. [redacted], the FBI continued to require the reporting of all third party errors to the FBI OGC as a potential IOB matter, even though only those errors that the FBI compounded would ultimately be reported to the IOB. In a letter to the IOB dated October 2, 2008, the FBI [redacted] a change in FBI policy that would require FBI personnel to report as a potential IOB matter only those third party errors that the FBI compounded (a modification that would drastically reduce the number of potential IOB matters requiring adjudication by the FBI OGC). On November 14, 2008, [redacted] the NSL-related compliance problems identified in the OIG's first NSL report. Nevertheless, FBI policy requires that case agents notify the FBI OGC of uncompounded third party errors for tracking purposes. Further, following [redacted] in August 2011, the FBI OGC (Cont'd.)

(described later in this chapter), we did not identify overcollections resulting from third party error as potential IOB violations unless the FBI compounded the error by using unauthorized information in the investigation or uploading unauthorized information into an FBI database.

B. NSL-Related Potential IOB Violations Reported to the FBI OGC

According to information the FBI provided to the OIG, between January 1, 2007, and December 31, 2009, FBI personnel reported 1,398 potential intelligence violations to the FBI OGC arising from the use of NSL authorities. In contrast, 85 potential intelligence violations were reported to the FBI OGC in 2006 and 26 were reported to the FBI OGC in 2003 through 2005.[93]

We believe that the substantial increase in the reporting of potential IOB violations in 2007 through 2009, as compared to 2003 through 2006, is largely attributable to the heightened awareness and oversight of the FBI's use of NSLs resulting from the OIG's previous NSL reviews. As we described in our second NSL report, we believe that our first NSL review focused the FBI's attention on its obligation to closely scrutinize NSLs for adherence to statutory requirements, examine information obtained in response to NSLs, and report potential violations to the FBI OGC.[94] The findings of our second NSL review reinforced the need for this focused attention, as have the NSL reviews conducted by the FBI's Inspection Division and the NSRs conducted jointly by the FBI OGC and NSD. Some of the potential IOB violations reported to the FBI OGC between 2007 and 2009 arose from matters specifically identified by our previous reviews or by the FBI's Inspection Division reviews and the Department's NSR program. In addition, some of the potential violations undoubtedly were reported as a result of the increased guidance and training provided to FBI personnel on these topics since our first report. For example, an opinion issued by the Office of Legal Counsel on November 5, 2008 concerning the scope of the term "subscriber information" as used in the ECPA NSL statute led to retroactive reporting of potential IOB violations.[95]

---

now provides a summary report to the IOB on a quarterly basis reflecting: (1) the total number of NSLs served during the quarter; (2) the total number of third party errors resulting from NSLs; (3) a description of the third party errors; and (4) the total number of third party errors compounded by the FBI.

[93] NSL I Report, 70; NSL II, 138.

[94] NSL II Report, 138.

[95] The OLC's November 2008 opinion concluded, among other things described elsewhere in this report, that the term "subscriber information" as used in the ECPA NSL (Cont'd.)

In our previous NSL reviews, we analyzed all of the NSL-related potential IOB violations that were reported to the FBI OGC in 2003 through 2005 and in 2006. In this review, we determined that most of the potential violations reported to the FBI OGC between January 1, 2007, and December 31, 2009, arose from facts that occurred before use of the NSL subsystem became mandatory in all FBI field divisions. We concluded that because the NSL subsystem significantly changed how the FBI generates NSLs and tracks the handling of NSL return data, pre-subsystem potential IOB violations would not be as instructive in assessing the FBI's progress in implementing our recommendations as potential violations that occurred after the implementation of the subsystem. We therefore focused our analysis in this report on the potential IOB violations that *occurred* between January 1, 2008, and December 31, 2009, rather than the potential violations that were *reported* to the FBI OGC during that same time frame.

Of the 1,398 NSL-related potential intelligence violations reported to the FBI OGC from January 1, 2007, through December 31, 2009, 398 appear to involve events that occurred between January 1, 2008, and December 31, 2009.[96] Of this number, the FBI OGC reported 112 potential violations to the IOB. We describe and analyze these 112 potential IOB violations below, as well as the 286 potential violations that the FBI OGC decided not to report to the IOB.

---

statute is limited to name, address, and length of service. Following the OLC opinion, in January and February 2009, the FBI OGC issued guidance to all CDCs directing field personnel to handle as an overcollection, and either destroy or return, any information in addition to name, address, and length of service obtained in response to subscriber-only ECPA NSLs. The guidance further instructed CDCs to report the matter as a potential IOB violation if the information in question was used in an investigation or uploaded into an FBI database.

[96] In 60 of the 1,398 NSL-related potential intelligence violations reported to the FBI OGC between 2007 through 2009, we were unable to determine from available documentation whether the potential violations arose from events that occurred between January 1, 2008, and December 31, 2009. We have excluded those potential violations from our analysis.

FIGURE 4.1
Summary of 398 NSL-Related Potential IOB Violations Reported to FBI OGC

Category of Potential IOB Violations	Potential IOB Violations Reported to the FBI OGC		Potential IOB Violations Reported to the IOB	
	FBI Error	Initial Third Party Error	FBI Error	Initial Third Party Error
Improper authorization	8	-	7	-
Improper request	29	-	22	-
Unauthorized collection	4	357	4	79
Total Potential IOB Violations Reported to the FBI OGC that occurred in 2008 - 2009			**398**	
Total Potential IOB Violations Reported to the IOB that occurred in 2008 - 2009			**112**	

C. NSL-Related Potential IOB Violations Reported to the IOB

The 112 NSL-related potential intelligence violations reported to the IOB arose from 34 matters reported to the FBI OGC.[97] In Figure 4.2 below, we provide a summary of the 34 matters and 112 potential IOB violations reported to the IOB by category during our review period.

[97] Six matters reported to the FBI OGC involved more than one potential violation. We calculated the number of potential violations in any given matter by counting the number of separate errors found. For example, if the FBI issued an improper NSL request by making a substantive typographical error in the NSL target's telephone number and then compounded that error by using or uploading into an FBI database unauthorized information obtained through the NSL request, we counted two separate potential IOB violations in one potential IOB matter. After reviewing a draft of the report, the FBI told the OIG that it would calculate this example as presenting one IOB matter, without counting the number of errors related to the same NSL request as separate violations. We do not find this difference in calculation method significant as long as each error is reported to the IOB, which appears to have been the case in 2008 and 2009 from the documentation we reviewed.

FIGURE 4.2
Summary of 112 NSL-Related Potential IOB Violations Reported to the IOB that occurred in 2008-2009 by Category

	Category of Potential IOB Violations	Number of IOB Matters	Number of IOB Potential Violations
Improper Authorization	NSL issued absent an open preliminary or full national security investigation	1	1
	Investigative file lacked predication to support the issuance of the NSL	1	5
	NSL lacked approval of an authorized SES official	1	1
	Total Improper Authorization	3	7
Improper Request	NSL contained a substantive typographical mistake affecting items such as target names, addresses, and telephone numbers (regardless of whether the NSL resulted in the receipt of unauthorized information)	17	21
	NSL requested information irrelevant to an authorized investigation	-	1
	NSL requested information beyond the scope permitted by statute or policy	-	-
	Total Improper Requests	17	22
Unauthorized Collection	FBI error identified above resulted in an unauthorized collection and the unauthorized information was used and/or uploaded into an FBI database		4
	Initial third party error resulted in unauthorized collection and the unauthorized information was used and/or uploaded into an FBI database	14	79
	Total Unauthorized Collection Used and/or Uploaded	14	83
	Total Potential IOB Violations Reported to the IOB	**34**	**112**

Twenty-two of the 29 NSL-related potential intelligence violations in Figure 4.2 that are categorized as improper authorizations and improper requests also resulted in unauthorized collections. We did not "double count" these matters by including them in the "unauthorized collection" category. However, additional violations were identified when the FBI compounded its initial error by using or uploading the unauthorized information into an FBI database, which it did in four instances. In the other 18 instances, the unauthorized collection was not compounded by the use or uploading of the unauthorized information.

Nature of the Potential Violations: Of the 112 NSL-related potential intelligence violations reported to the IOB, 21 involved a substantive typographical mistake in an NSL causing the FBI to request and in some cases receive information not relevant to an authorized investigation. As noted above, in four such instances, the FBI compounded its initial

typographical mistake by uploading the irrelevant information into an FBI database.[98]

Another 79 potential IOB violations involved unauthorized collections caused by initial third party errors. In each instance, the NSL return data constituted an overcollection that included information the provider was prohibited by statute to disclose to the FBI. The FBI compounded the initial third party error by using or uploading the unauthorized information into an FBI database. Sixty-six of these 79 unauthorized collections occurred in one matter after the case agent failed to recognize that a third party provider produced telephone toll billing records for a telephone number not requested in the NSL and not relevant to the investigation. Compounding the initial third party error, the case agent uploaded the records into an FBI database and issued 5 new NSLs, each requesting telephone subscriber information for 13 telephone numbers appearing in the records mistakenly produced by the provider.

The remaining 8 potential violations reported to the IOB concerned the following 3 matters:

- An FBI field division served an NSL request pursuant to the ECPA after the originating field division closed the authorized investigation.
- An FBI field division issued five NSL letters pursuant to the ECPA from a preliminary investigation that lacked predication. Before issuing the NSLs, the field division opened a preliminary investigation that was initially classified as a computer intrusion investigation and later reclassified as a "technical support to terrorism investigation." According to the FBI OGC's written adjudication of this potential IOB matter, FBI policy required that an investigation classified as "technical support to terrorism investigation" must have as its predicate a concurrent counterterrorism investigation. At the time the field division issued the five NSLs, however, a predicate counterterrorism investigation had not been opened. The FBI OGC determined that the matter should be reported to the IOB because issuing

[98] In a fifth instance, an FBI field division did not compound its initial typographical mistake by uploading the irrelevant information into an FBI database for investigative purposes, but it did include the information in the electronic communication reporting the potential IOB matter to the FBI OGC, which was uploaded into the FBI's Automated Case Support database (ACS). We counted one potential IOB violation in this matter for the improper request resulting from the typographical mistake but did not count another potential violation for the inclusion of the irrelevant information in the reporting EC that was uploaded into ACS. Nevertheless, the FBI OGC should remind personnel not to include unauthorized information in the reporting EC.

the NSLs from an unpredicated investigation violated the ECPA and Attorney General Guidelines.

- An FBI field division analyst altered the date range specified in an NSL for financial records before serving the NSL by crossing out the beginning date of January 1, 2006, and substituting a new date of September 17, 2004. The analyst did not obtain approval from the SAC of the originating field division for the changed request. In response to the altered NSL, the FBI received records that were outside the date range requested by the originating division and not relevant to the investigation. According to its adjudication memorandum, the FBI OGC determined the matter should be reported to the IOB because an FBI error resulted in the overcollection of information not relevant to the investigation. Based upon the information provided in the reporting EC and in the written adjudication, we concluded that the facts in this matter gave rise to two separate violations: issuing an NSL request without the approval of an SAC and requesting information not relevant to an authorized investigation.

U.S. Person Status: We sought to determine whether the subject of the investigation and the target of the NSL in these 112 NSL-related potential IOB violations were U.S. persons.

- In 96 potential violations, the investigative subject was, or was presumed to be, a U.S. person, and in 16 potential violations the subject was a non-U.S. person.
- Similarly, in 96 potential violations, the NSL target was, or was presumed to be, a U.S. person, and in 16 potential violations the target was a non-U.S. person

Timeliness of Reporting: As described above, the 112 NSL-related potential intelligence violations reported to the IOB arose from 34 matters reported to the FBI OGC. In this review, we attempted to determine the timeliness of the reporting of these 34 matters by examining the number of days between (1) occurrence and discovery, (2) discovery and reporting to the FBI OGC, and (3) reporting to the FBI OGC and the FBI OGC's adjudication.

First, we calculated the time it took for FBI personnel to discover or identify the potential IOB matter. We could not determine the relevant time period for 9 of the 34 IOB matters because the electronic communication reporting the matter to the FBI OGC and the FBI OGC's adjudication memorandum did not indicate the date of the occurrence or the date of the discovery, or both. For the remaining 25 matters, we determined that the

average time period between the date of the occurrence and the date of discovery was 72 days.[99]

Second, we calculated the time it took for FBI personnel to report the potential IOB matter to the FBI OGC. We could not determine the relevant time period for 3 of the 34 matters because the electronic communication reporting the matter to the FBI OGC and the FBI OGC's adjudication memorandum did not indicate the date the matter was discovered. For the remaining 31 matters, we determined that the average time between the date of discovery and the date the matter was reported to the FBI OGC was 34 days.

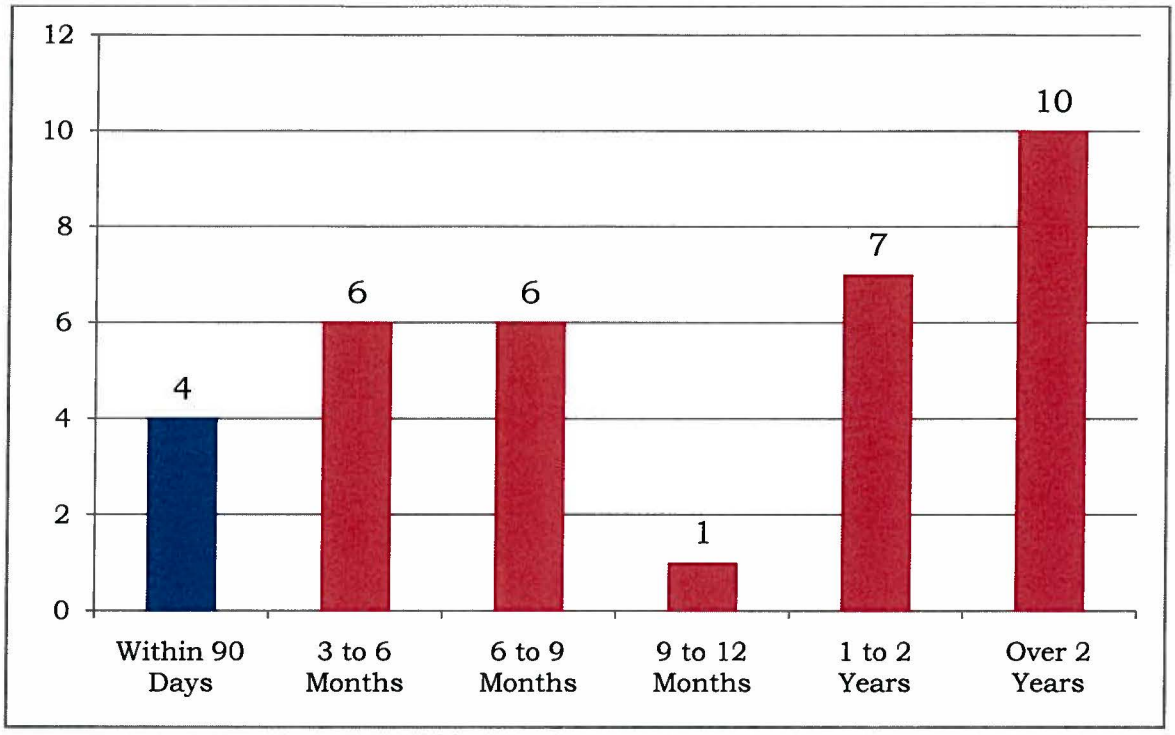
We also evaluated how often FBI personnel reported these 28 potential IOB matters to the FBI OGC within the time requirements set forth in FBI policy. As described in Section I.B.1, above, the FBI's April 2009 IOB policy requires that potential IOB matters be reported to the FBI OGC within 30 days of discovery. The FBI's previous IOB guidance memoranda, which applied to potential IOB matters reported before April 2009, required that such matters be reported within 14 days. Applying the requisite time requirements to the 31 matters, we found that FBI personnel reported 24 of 31 potential IOB matters, or 77.4 percent, to the FBI OGC in a timely manner.

Finally, we calculated the time it took for the FBI OGC to issue its adjudication. We determined that the average time between the date FBI personnel reported the 34 potential IOB matters to the FBI OGC and the date the FBI OGC issued its adjudication was 427 days, with a range between 35 days and 919 days. None of these matters concerned a "significant or highly sensitive" matter that should have been reported to the IOB immediately. These matters were therefore subject to the quarterly reporting requirement set forth in the July 17, 2008, reporting criteria jointly issued by the IOB and DNI. As illustrated in Figure 4.3 below, we evaluated how many of these matters the FBI OGC adjudicated within 90 days from the date of the report to the FBI OGC and determined that the FBI OGC did so in 4 of the 34 matters, or in 11.8 percent of the matters.

---

[99] For potential IOB violations resulting from an FBI error in the NSL, we used the date the NSL was served by the serving field division, if available, as the date of occurrence in our calculation. In instances where the service date was unavailable, we used the date the NSL was approved or issued in the NSL subsystem. For potential IOB violations resulting from third party error in the NSL return data, we used the date the FBI received the NSL return data as the date of occurrence.

FIGURE 4.3: Timeliness of FBI OGC's Adjudication of NSL-Related Potential IOB Violations Reported to the IOB



Remedial Actions Taken: Of the 112 possible NSL-related intelligence violations reported to the IOB, 106 resulted in the FBI receiving an unauthorized collection.[100] We examined these matters to determine whether the FBI handled the unauthorized collections in conformity with FBI policies and procedures.

In 22 of the 106 instances, the FBI did not use or upload the unauthorized information before discovering the potential violation, sequestering the information, and reporting the matter to the FBI OGC. In its adjudication memoranda, the FBI OGC instructed the field divisions to destroy, redact, or return the hard copies to the provider unless they had already done so. In a few instances, the FBI OGC also advised that the field division could issue a new NSL for the unauthorized information if that information was relevant to an authorized investigation and within the permissible scope of the applicable statute.

In the remaining 84 instances, the FBI uploaded or used the unauthorized information before discovering the potential violation and

[100] In six instances, all involving a substantive typographical error in an NSL, the provider did not return results to the FBI.

reporting the matter to the FBI OGC. After discovery, the field divisions appropriately sequestered the information and reported the potential violations to the FBI OGC. The FBI OGC instructed the field divisions to purge the unauthorized information from FBI databases and destroy, redact, or return the hard copies to the provider unless they had already done so. In a few instances, the FBI OGC also advised that the field could issue a new NSL for the unauthorized information if that information was relevant to an authorized investigation and within the permissible scope of the applicable statute.

Comparison of NSL-Related IOB Violations in 2008 and 2009 to Those Described in Previous OIG Reviews: The FBI OGC reported more NSL-related IOB violations to the IOB for activity that occurred in 2008 and 2009 (112 reported violations) than it had reported in 2003 through 2005 and in 2006.

In our first NSL report, we found that the FBI OGC reported 19 NSL-related IOB violations to the IOB in 2003 through 2005.[101] The violations included three instances where the FBI issued NSLs from cases that lacked the appropriate authorization, two instances where the FBI obtained telephone toll billing records or financial records without issuing an NSL, and one instance where the FBI issued an NSL seeking a full credit report in a counterintelligence case without a counterterrorism nexus. The violations also included 13 unauthorized collections, the majority of which were the result of FBI error.

In our second NSL report, we found that the FBI OGC reported 34 NSL-related IOB violations to the IOB in 2006.[102] Twenty-nine of those matters, or 85 percent, involved unauthorized collections. Fifteen of the unauthorized collections were the result of FBI error such as substantive typographical errors in the NSLs. The remaining 14 unauthorized collections were the result of third party error such as providers producing records that were different than or beyond the scope of what the FBI requested in the NSL. Three other matters reported to the IOB concerned NSLs issued from cases that lacked the appropriate authorization, one concerned the service of an ECPA NSL in a manner that was deemed improper under the pertinent NSL statute, and one involved unauthorized investigative activity during a lapse in authorization.

---

[101] NSL I Report, 71-72.

[102] NSL II Report, 140-143.

D. OIG Analysis of the Reporting of Potential IOB Violations to the IOB

Our examination of the 112 NSL-related potential IOB violations reported to the IOB did not reveal deliberate violations of NSL statutes, Attorney General Guidelines, or internal FBI policy. Although 33 of these violations resulted from initial FBI errors, we found that most of the errors were typographical mistakes in the telephone number, e-mail address, or name identified in the NSL. In the 79 matters where the FBI compounded an initial third party error through the use or uploading of unauthorized information, our examination did not reveal any reasons for the FBI's use or uploading of the information other than the failure of the case agent to identify the unauthorized collection in a timely manner.

We do not draw a negative inference about the FBI's compliance with NSL authorities from the fact that the FBI OGC reported 112 NSL-related IOB violations to the IOB for activity that occurred in 2008 and 2009, as compared to 19 in 2003 through 2005 and 34 in 2006. As we concluded in our second NSL report about the increase in IOB reporting between 2003 and 2006, we believe that the increase in IOB reporting after 2006 is more likely a reflection of the FBI's increased attention on NSL requirements and the obligation to report potential violations to the FBI OGC than an indication that the FBI committed more intelligence violations in its use of NSLs in 2008 and 2009.[103]

Further, a comparison of the violations reported to the IOB during the different time frames indicates that the nature of the NSL-related IOBs has not changed significantly since 2003. The vast majority of the matters that the FBI reported during each of our review periods concerned potential IOB violations caused by substantive typographical errors in the NSLs or by initial third party error.

We found that FBI personnel reported to the FBI OGC in a timely manner most of the 34 matters identifying 112 NSL-related potential violations that the FBI OGC ultimately reported to the IOB. In the 28 matters for which we were able to discern the relevant time frames, FBI personnel discovered the potential violations within an average of 33 days from their occurrence, and reported 22 of 28 potential IOB matters, or 78.6 percent, to the FBI OGC in a timely manner under then applicable FBI policy.

A greater challenge for the FBI was in the adjudication of the reported matters. As noted above, the FBI OGC took an average of 428 days, or

---

[103] NSL II Report, 138.

about 14 months, to report the 34 matters to the IOB. In the most egregious example, the FBI OGC took 919 days, or about 2 and one half years, to adjudicate a matter involving what appeared to be a relatively straightforward unauthorized collection.

We sought to determine the cause of the slow pace of these FBI OGC adjudications. Steven Siegel, who was the Deputy General Counsel of the NSLB from September 2009 to April 2012 and a supervisor in NSLB before he became Deputy, told us that the FBI OGC was inundated in 2007 and 2008 with the reporting of more than 4800 potential IOB violations, the majority of which were not NSL-related. According to Siegel, a shortage of resources in NSLB to handle this influx resulted in a backlog of pending adjudications. Although NSLB has worked through the backlog by assigning adjudications to all NSLB attorneys, in September 2012 there were 44 matters reported to the FBI OGC between 2007 through 2009 awaiting adjudication. Siegel told us that NSLB has not had enough attorneys to address the backlog and those attorneys who are available have competing priorities.

Similarly, the Assistant General Counsel in NSLB who serves as the primary point of contact on potential IOB violations told us that current operational needs have taken priority over preparing adjudications on past violations. She also told us that inconsistency and incompleteness in the reporting documents from the field further drains NSLB resources because adjudications often require multiple follow-ups with the field to obtain missing information.

To assist in the management of the IOB reporting process, the FBI has developed a new subsystem in its FISA Management System with assistance from the same contractors who developed the NSL subsystem. The new IOB subsystem, which the FBI implemented in all field divisions in November 2012, automates the work process of reporting potential IOB violations to the FBI OGC by prompting agents in the field through the required elements of the report before transmittal of the report to the FBI OGC. The Assistant General Counsel who serves as the primary point of contact on potential IOB violations told us that the IOB subsystem is expected to improve the completeness and consistency in reporting and, therefore, improve the timeliness of adjudications. She said she also expects that the new subsystem will provide the FBI with a better management tool for tracking potential IOB violations as they move through the reporting process and generating statistical reports.

While the IOB subsystem is an improvement in the FBI OGC's management of the IOB reporting process, we believe it will not address the main causes of the FBI OGC's slow pace in reporting potential intelligence violations to the IOB. The FBI should take additional steps to address the

substantial delays in adjudication caused by limited resources and competing priorities.[104]

E. NSL-related Potential IOB Violations Not Reported to the IOB

In 2008 and 2009, FBI personnel reported 286 NSL-related potential intelligence violations to the FBI OGC that the FBI OGC decided not to report to the IOB. The 286 NSL-related potential intelligence violations arose from 195 matters reported to the FBI OGC. Of the 286 potential IOB violations, 277 involved reports by the field of possible or suspected unauthorized collections caused by an initial third party error. The FBI OGC decided not to report 265 of these 277 potential violations to the IOB because the FBI did not compound the initial third party error through the use or uploading of unauthorized information.[105] The FBI OGC decided not to report the other 12 potential violations because the FBI OGC concluded that the information was properly obtained by the FBI.

FBI personnel reported 9 of the 286 potential IOB violations to the FBI OGC as having resulted from potential FBI errors. These potential FBI errors involved the following five matters:

- A field division reported that, after the expiration of the preliminary investigation, a case agent uploaded telephone toll records received in response to an ECPA NSL into the FBI's Telephone Applications database and reviewed and analyzed the information. The FBI OGC determined that the matter was not a reportable IOB violation, finding that: (1) the FBI properly served the NSL; (2) the FBI reviewed legally obtained NSL results; and (3) under then-controlling Attorney General Guidelines, the FBI was permitted to review NSL results without opening a preliminary or full investigation. According to the FBI OGC, because the NSL was properly issued during a valid preliminary investigation and the agent "merely" reviewed and

---

[104] After reviewing the draft of this report, the FBI told the OIG that it had created new time requirements for the preparation and review of adjudication memoranda, and that NLSB attorneys now receive an e-mail notification when the requirements are not met. According to the FBI, these additional steps have reduced the average time taken to adjudicate potential IOB matters. We believe the FBI should continue these measures and consider additional steps to reduce adjudication time.

[105] As described in footnote 92 above, on August 1, 2007, [redacted] the FBI OGC to report to the IOB all third party errors that the FBI compounded through the FBI's use of the inappropriately provided information or the uploading of the information onto an FBI database. [redacted], the FBI stopped reporting uncompounded third party errors to the IOB.

analyzed the NSL results and did not take further investigative action after the expiration of the preliminary investigation, the matter did not require a report to the IOB.

- A field division reported an unauthorized collection in a counterintelligence investigation that may have been caused by the format of the NSL generated in the NSL subsystem. The report to FBI OGC noted that the provider produced the financial records requested in the RFPA NSL along with the records of another, unrelated account having the same address as the target of the NSL. The field division questioned whether the provider misinterpreted the request because the "address" portion of the NSL was separated from the name and date of birth of the target of the NSL. The FBI OGC determined that the matter was not a reportable IOB violation, finding that the provider produced records beyond the scope of the request, and the FBI did not compound the provider's error by using or uploading the information.
- A field division reported an unauthorized collection in a counterterrorism investigation caused by the case agent mistakenly using the wrong social security number in an NSL request. The NSL sought the full credit report of the subject of the investigation, but the case agent mistakenly included the social security number of the subject's spouse in the identifying information in the NSL. As a result of the mistake, the provider produced the full credit report of the subject's spouse, not the full credit report of the subject. The FBI OGC determined that the matter was not a reportable IOB violation because the spouse's credit report was relevant to the investigation at the time the FBI issued the NSL. According to the FBI OGC, evidence in the FBI's possession indicated that the spouse may have been engaged in "nefarious" financial transactions on behalf of the investigative subject.
- A field division reported that it discovered that the approval EC supporting two ECPA NSLs that sought electronic communication transactional records on a total of five separate e-mail accounts contained inaccurate information. The report stated that the approval EC misidentified the database from which it was determined that the targets of the NSLs had e-mail contact with the subject of the underlying counterterrorism investigation. The FBI OGC determined that the NSLs did not present reportable IOB violations because the mistake in the approval EC did not undermine the predication or justification for the NSLs or the relevance of the records requested and was

not pertinent to the certifications of relevance and non-disclosure made by the approving official.[106]

- A field division reported that it requested subscriber information and toll billing records for two telephone numbers believed to be used by the investigative subject and, upon receipt and review of the return data, discovered that one of the telephone numbers was used by an individual unrelated to the investigation. The FBI OGC determined that the matter was not a reportable IOB violation because, at the time the NSL was served, the field division had reason to believe the subscriber of the telephone number was the investigative subject. According to the FBI OGC, because relevance is determined at the time an NSL is served upon a carrier, the FBI lawfully acquired the information on both telephone numbers. Nevertheless, the FBI OGC instructed that the records of the individual unrelated to the investigation remain sequestered with the Chief Division Counsel (CDC) or be destroyed.

Timeliness of Reporting: As described above, the 286 NSL-related potential intelligence violations that were not reported to the IOB arose from 195 matters reported to the FBI OGC. We determined that FBI personnel reported 123 of the 195 matters within the requisite 14-day or 30-day time requirements set forth in FBI policy. We could not determine how long it took to report 32 of the 195 matters because the electronic communication reporting the matter to the FBI OGC and the FBI OGC's adjudication memorandum did not indicate the date the matter was discovered. The remaining 40 of the 195 matters were not reported to the FBI OGC in a timely fashion, with a range between 15 and 287 days. The average time period between the date of discovery and the date of reporting to the FBI OGC for all but the 32 matters missing such information was 17 days.

We also determined the time it took for the FBI OGC to issue its adjudication memorandum in each matter. We found that the average time between the date FBI personnel reported the 195 potential IOB matters to the FBI OGC and the date the FBI OGC issued its adjudication was 233 days, with a range between 25 and 942 days.

Remedial Actions Taken: Of the 277 potential violations reported to the FBI OGC as initial third party errors, we found that the FBI handled 276 in conformity with FBI policies and procedures by identifying and sequestering the information in question with the CDC. With respect to the

---

[106] Because the error affected five requests for electronic communication transactional records, we counted the matter as containing five potential IOB violations. Thus, we counted nine potential IOB violations in five matters alleging FBI error.

remaining reported initial third party error, we found that the case agent failed to identify and sequester an unauthorized collection. The unauthorized collection was discovered as a result of an internal review conducted by the FBI's Inspection Division.

According to the FBI OGC's adjudication memorandum for each of the 277 potential violations, the FBI took the following actions after identifying an initial third party error and sequestering the information in question:

- In 52 instances, the FBI field division took action to redact, destroy, issue another NSL, or return the unauthorized information before the FBI OGC issued its adjudication.
- In 203 instances, the FBI OGC appropriately instructed in its adjudication that the field division destroy, redact, or return the unauthorized information, unless they had already done so. In some cases, the FBI OGC also advised the field division that they could issue a new NSL requesting the unauthorized information if that information was relevant to an authorized investigation and within the permissible scope of the applicable NSL statute.
- In 12 instances, the FBI OGC determined that the information was properly obtained by the FBI and therefore did not require remedial action.
- In 10 instances, the FBI OGC instructed the field division to continue sequestration of the NSL results pending a legal opinion from the OLC on certain issues pertaining to the scope of the ECPA NSL statute. In November 2008, the OLC issued its opinion, which concluded, among other things described elsewhere in this report, that the term "subscriber information" in the NSL statute is limited to name, address, and length of service. Following the OLC opinion, in January and February 2009, the FBI OGC issued guidance to all CDCs directing the field to handle as an overcollection and either destroy or return any information in addition to name, address, and length of service obtained in response to subscriber-only ECPA NSLs.

The remaining 9 of the 286 potential violations reported to the FBI OGC involved the possibility of FBI error. Only three of the possible FBI errors required remedial action. In the first instance, unauthorized information was immediately identified and sequestered with the CDC. In the second instance, the case agent discovered the receipt of unauthorized information during a routine case file review and sequestered the information with the CDC. In its adjudication memoranda for these two matters, the FBI OGC appropriately instructed the field divisions to destroy

or return the information to the provider. The FBI OGC also advised the field division in the first matter that it could issue a new NSL requesting the information if that information was relevant to an authorized investigation. In the third instance, the irrelevance of the information obtained by the FBI was discovered only after the information was uploaded into the FBI's Telephone Applications database. The field division removed the information from the database and sequestered the information with the CDC. In its adjudication of this matter, the FBI OGC instructed that the irrelevant information remain sequestered with the CDC or be destroyed.

F. OIG Analysis of NSL-related Potential IOB Violations Not Reported to the IOB

Our review showed that the FBI OGC decided not to report 286 of the 398 NSL-related potential intelligence violations to the IOB. Most of the 286 concerned reports of uncompounded third party errors. As described above, the FBI stopped reporting uncompounded third party errors to the IOB after August 2007 and notified the IOB that it intended to stop requiring the reporting of those matters to the FBI OGC as potential IOB violations. Because these changes in FBI policy [redacted], we found unremarkable the FBI OGC's determinations not to report uncompounded third party errors to the IOB.

We believe 11 of the 286 potential intelligence violations not reported to the IOB warrant reconsideration. In 8 of these 11 matters, we disagreed with the FBI OGC's decision not to report the potential intelligence violation to the IOB. In the first matter, the case agent mistakenly used the wrong social security number in an NSL request, resulting in the receipt of a full credit report of someone other than the target of the NSL, specifically, the target's spouse. In its decision not to report the matter to the IOB, the FBI OGC reasoned that the mistake did not result in a violation of FCRA because the full credit report provided by the credit agency was relevant to the investigation at the time the FBI issued the NSL.

We found, however, that the FBI OGC's analysis should not have ended with this after-the-fact relevance determination. The applicable statute required that the NSL contain the certification of a designated supervisory official that the requested records were necessary for an investigation of, or intelligence or counterintelligence activities or analysis related to, international terrorism. 15 U.S.C. § 1681v. According to the report from the field division and the FBI OGC's adjudication memorandum, the SAC who signed this NSL approved and certified a request for records concerning the named target in the NSL, not records of the target's spouse. We therefore concluded that the invalid certification was a statutory violation that the FBI OGC should have reported to the IOB, not merely a violation of FBI policy as determined by the FBI OGC.

In the second matter, we disagreed with the decision not to report a potential intelligence violation concerning the receipt and subsequent upload into ACS of an additional contact number received in response to an NSL request for telephone subscriber information. The FBI OGC reasoned that while the subscriber's additional contact information was beyond the scope of the request, "additional contact information falls under the subscriber information legally releasable under ECPA and the release of that information is not considered an over-production." However, consistent with the finding in the November 2008 OLC opinion that the scope of subscriber information under the ECPA is limited to name, address, and length of service, we concluded that the FBI's receipt of the additional phone number constituted an unauthorized collection and the subsequent uploading of that information into an FBI database compounded this unauthorized collection, thereby resulting in an IOB that should have been reported.[107]

We disagreed with the decision not to report six potential intelligence violations in four matters involving the FBI's request for and receipt of records for additional telephone numbers "associated" with the telephone number identified in the NSL request.[108] "Associated" telephone numbers are additional telephone numbers subscribed under the same account as the telephone number identified in the NSL request, such as in joint or "family plan" accounts. Four of the six potential violations concerned the receipt of toll billing records for additional telephone numbers that were associated with the targeted number, and two potential violations concerned the receipt of subscriber information related to an additional telephone number associated with the targeted number.

- In one matter presenting three potential IOB violations, the field division received the toll billing records of the target of the NSL request as well as three additional sets of toll billing records for telephone numbers not specifically identified in the NSL. The field division later learned that the target's telephone number was one of multiple telephone numbers assigned to an account subscribed to by the target's mother. In other words, because the telephone number believed to be used by the NSL target was part of a family plan of telephone numbers subscribed to by the target's mother, the provider produced the toll billing records for the other numbers assigned to the mother's account. According

[107] The FBI OGC has advised the OIG that it has reconsidered its determination in this matter and reported this apparent violation to the IOB on July 8, 2013.

[108] We also discuss in Chapter Five the FBI's practice of requesting and receiving toll billing records for telephone numbers "associated with" the number targeted in the NSL request.

to its adjudication memorandum, the FBI OGC decided not to report this matter to the IOB because the NSL included a request for the records of all telephone numbers associated with the targeted account or account-holder.

- In another matter, the field division received the toll billing records of the target of the NSL request as well as the toll billing records of an additional number not specifically identified in the NSL. The field division later learned that the provider identified the additional telephone number as belonging to the target of the NSL. The additional number was located in a lab at an academic institution where the target worked, and where students and professors other than the target had access to and may have used the telephone. The FBI OGC decided not to report the matter to the IOB because the additional telephone number was assigned to or associated with the target of the NSL request.
- In a third matter, the field division received telephone subscriber information for the target of the NSL request and received an additional telephone number and social security number. The reporting documentation and the FBI OGC's adjudication memorandum did not identify the individual to whom the additional telephone number and social security number belonged. According to the FBI OGC's adjudication memorandum, the FBI did not know whether the additional telephone number was given to the provider by the subscriber of the account as an alternate contact number or whether the additional number was another telephone number "associated" with the targeted telephone number through a joint or family plan account. The FBI OGC concluded that receipt of an alternate contact number would constitute an unauthorized collection, consistent with the finding in the November 2008 OLC opinion that the scope of subscriber information under the ECPA is limited to name, address, and length of service, but that receipt of "associated" numbers would not constitute an unauthorized collection because the NSL letter requested the production of alternate subscriber information associated with the account. Based on this reasoning, the FBI OGC decided not to report the matter to the IOB, stating that even assuming the additional information constituted an unauthorized collection, the field division did not compound the error by using or uploading the additional information.
- In the final matter, the field division received telephone subscriber information for the target of the NSL request and telephone subscriber information for an additional telephone

number. According to the FBI OGC's adjudication memorandum, the provider identified the additional telephone number as belonging to the target of the NSL. According to the memorandum, the FBI OGC decided not to report the matter to the IOB because the NSL requested "associated" records and because Section 2709 "permits the carrier to determine the scope of the request and provide at its discretion those records pertaining to all telephone numbers associated with the targeted account or account-holder in the NSL...."

As described above, in its adjudication memorandum for each of these matters, the FBI OGC determined not to report the potential violation to the IOB on the ground that the "associated" records were responsive to the NSL request at issue. In one matter, the FBI OGC also stated, without citing specific statutory language or case law, that Section 2709 gives the provider discretion to determine the scope of the FBI's request and provide records of all telephone numbers associated with the targeted account or account-holder in the NSL. In the other adjudication memoranda, the FBI OGC provided no justification for the collection of this information other than the fact that language in the NSL requested the information.

The FBI's templates for ECPA NSLs seeking toll billing records or telephone subscriber information include an attachment stating that the recipient of the letter "should determine whether your company maintains the following types of information which may be considered by you to be toll billing records in accordance with" Section 2709. The types of information identified include [redacted] Significantly, the FBI routinely includes this request in its ECPA NSLs without requiring any determination and certification by the SAC that the additional records are relevant to an authorized national security investigation.

As described in more detail in the next chapter, we believe that the ECPA requires the FBI to first determine whether the records of associated telephone numbers are in fact relevant to a national security investigation before seeking such records directly through an NSL. We therefore disagreed with the decision not to report these six potential violations to the IOB.[109]

---

[109] After reviewing the draft of this report, the FBI told the OIG that in response to our concern about the FBI's practice of requesting associated records without first

(Cont'd.)

Finally, in the remaining three matters, we concluded that the FBI OGC failed to consider significant legal issues before deciding not to report the potential violations to the IOB. We believe these questions should have been resolved before making a decision not to report the potential violations to the IOB.

In one of these matters, the FBI received date of birth information for the subscriber of the targeted account in response to a request for subscriber information and electronic communication transactional records. According to the FBI OGC's adjudication memorandum, the records received in response to the NSL, including the date of birth information, were uploaded into an FBI database. The memorandum stated without citation to any legal authority that the matter was not reportable to the IOB because the FBI may receive date of birth information in response to an NSL seeking electronic communication transactional records. The FBI OGC provided similar guidance in an *NSL Collection Chart* disseminated to field divisions in late 2010. The *NSL Collection Chart* describes the FBI OGC guidance on whether FBI personnel may retain, upload, and use specific categories of information received in response to each type of NSL. This guidance states – without citation to any legal authority – that the FBI may receive date of birth and social security number information in response to NSL requests for electronic communication transactional records to the extent the information is maintained by the provider as part of its electronic communication transactional records.

The NSL statute does not expressly permit the FBI to request subscriber information other than name, address, and length of service, and it is unclear whether "electronic communication transactional records" as used in 18 U.S.C. § 2709(a) and "toll billing records" as used in 18 U.S.C. § 2709(a) and (b) include anything other than records of incoming or outgoing communications. Until this legal question is resolved, we are unable to agree with the FBI OGC's decision not to report this potential intelligence violation to the IOB. The Department has sought an amendment to Section 2709 that would [redacted] Further, as we describe in greater detail in the next chapter, we believe that any efforts by the Department to bring about a legislative amendment to Section 2709 should seek to clarify whether the FBI may obtain the personal information of a subscriber other than name, address, and length of service – including date of birth, social security number, and credit card information – in response to an NSL

---

determining and certifying the relevance of those records to an authorized national security investigation, the FBI will reconsider its policies relating to this issue.

requesting toll billing records. Because legislative action may take some time, we also believe that the Department should include this issue in a request for a legal opinion from the OLC so that the FBI will have authoritative guidance in the interim.[110]

In a second matter, the FBI received records in response to an NSL during a preliminary investigation, but did not upload and review the records until after the investigation had expired. The FBI OGC decided not to report this as a potential intelligence violation. In the adjudication memorandum, the FBI OGC stated that since the FBI properly served the NSL for toll billing records before the expiration of the investigation, the FBI may review and analyze the results after the expiration of the investigation. For reasons we describe more fully in Chapter Five, we believe the FBI should consider implementing a policy that would require agents, in consultation with OGC attorneys, to carefully balance the privacy interests of the individual against the potential for future investigative value before permitting the uploading into FBI databases of NSL results received after a case has been closed or after the authority for the investigation has expired.

In the third matter, the FBI received information, including the NSL target's date of birth and six telephone numbers, in response to an NSL requesting limited credit information under Sections 1681u(a) and (b) of the FCRA. After receiving this information, the FBI uploaded it into an FBI database.

As noted earlier in this report, Section 1681u(a) of the FCRA permits the FBI to request through an NSL the names and addresses of all financial institutions associated with the NSL target. Section 1681u(b) permits the FBI to request through an NSL the consumer-identifying information of the NSL target, limited to name, address, former addresses, places of employment, and former places of employment. The request or receipt of a consumer's date of birth, social security number, and telephone numbers is not authorized under either section.

Despite receiving information outside the scope of its Section 1681u request, the FBI OGC decided not to report the matter to the IOB as a potential violation. In the adjudication memorandum describing its decision, the FBI OGC stated that a reasonable interpretation of the FCRA is that a carrier may voluntarily provide the FBI with dates of birth and

---

[110] After reviewing the draft of this report, the FBI told the OIG that it is the FBI OGC's opinion that the FBI may receive date of birth information in response to an NSL request under Section 2709(b)(1) to the extent the provider maintains the information as part of its toll billing records in the ordinary course of business. However, the FBI agreed that the statute is unclear and that it would reconsider, as a matter of policy, whether to continue to obtain dates of birth and social security numbers under Section 2709(b)(1).

telephone numbers because the FCRA does not protect this information from disclosure.

However, the FCRA contains a specific provision, 15 U.S.C. § 1681f, governing the voluntary disclosure of consumer identifying information to government agencies. This provision states:

> Notwithstanding the provisions of section 1681b of this title, a consumer reporting agency may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, and former employment, to a government agency.[111]

Courts addressing the application of Section 1681f have observed that this provision limits the scope of consumer identifying information that a consumer reporting agency may disclose to a government agency to name, address, former addresses, places of employment, or former employment unless the government agency compels production through legal process specified in Section 1681b.[112] Thus, Section 1681f appears to prohibit the voluntary disclosure to the FBI of a consumer's date of birth or telephone number.

The FBI OGC's adjudication memorandum made no mention of Section 1681f. Instead, it cited two district court cases, *Individual Reference Servs. Group, Inc.* v. *Fed. Trade Comm'n*, 145 F. Supp. 2d 6, 17 (D.D.C. 2001), *aff'd* 295 F.3d 42 (D.C. Cir. 2002), and *Dotzler* v. *Perot*, 914 F. Supp. 328, 330-31 (E.D. Mo. 1996), *aff'd* 124 F.3d 207 (8th Cir. 1997), *cert. denied*, 522 U.S. 1148 (1998), for the proposition that so-called "credit header" information falls outside the FCRA's definition of a "consumer report," and thus that the FCRA does not regulate the dissemination of

---

[111] Section 1681b provides that a consumer reporting agency may furnish a consumer report pursuant to a court order or grand jury subpoena. As originally enacted, government access to consumer information held by a consumer reporting agency required a court order under Section 1681b or voluntary disclosure under Section 1681f. *See* Pub. L. No. 91-508 (1970). In 1989, Congress added grand jury subpoena authority to Section 1681b. *See* Pub. L. No. 101-73 (1989). Congress later added NSL authority for the FBI in Section 1681u in 1996 and in Section 1681v in 2001. *See* Pub. L. No. 104-93 (1996), Pub. L. No. 107-56 (2001).

[112] *See, e.g., In re Gren*, 633 F.2d 825, 826-27 (9th Cir. 1980); *Fed. Trade Comm'n* v. *Manager, Retail Credit Co.*, 515 F.2d 988, 990, 994 (D.C. Cir. 1975); *Soghomonian* v. *United States*, 278 F. Supp.2d 1151, 1163-64 (E.D. Cal. 2003), *vac'd on other grounds*, 2005 WL 1972594 (E.D. Cal. Jun. 20, 2005); *Edgar* v. *Reich*, 881 F. Supp. 83, 86 (D. Mass. 1995); *In re Grand Jury Subpoena to the Credit Bureau of Greater Harrisburg*, 594 F. Supp. 229, 232 (M.D.Pa. 1984); *In re Grand Jury Subpoena Duces Tecum Concerning the Credit Bureau of Ga.*, 498 F. Supp. 1174, 1176-77 (N.D. 1980); *United States* v. *Lake County Nat'l Bank*, 1975 WL 548 (N.D. Ohio Mar. 18, 1975).

credit header information.[113] Relying upon these cases, the FBI OGC concluded that it was lawful for the consumer reporting agency to voluntarily provide the FBI with credit header information including the target's date of birth and six telephone numbers because this information is not a "consumer report."

However, neither *Dotzler* nor *Individual Reference* addressed whether the FCRA limits the scope of consumer identifying information that a consumer reporting agency may voluntarily disclose to a government agency. Indeed, neither case addressed Section 1681f, its legislative history, or the court opinions describing its application.[114]

The FBI OGC considered this legal question as early as September 2010, 10 months before the FBI OGC's adjudication of this matter. [redacted]

[redacted]

---

[113] "Credit header" information is identifying information about a consumer that typically appears at the top of a consumer report, such as name, address, social security number, and telephone numbers. *See Individual Reference,* 145 F. Supp. 2d at 14.

[114] *Individual Reference* rejected a challenge brought by Trans Union, LLC, and Individual Reference Services Group, Inc., to Federal Trade Commission (FTC) regulations implementing statutory restrictions on a financial institution's disclosure of "nonpublic personal information" to a nonaffiliated third party. The plaintiffs argued, among other things, that the FTC's regulations impermissibly conflicted with the FCRA because the regulations placed restrictions on a consumer reporting agency's use and disclosure of credit header information. *See* 145 F. Supp. 2d at 34-39. The parties in the case had stipulated that credit header information is not part of a "credit report" subject to privacy protection under the FCRA. The plaintiffs argued that because the FCRA does not regulate the disclosure of credit header information, and because the FTC regulations had a savings clause providing that nothing in the statute should be construed to modify, limit, or supersede the FCRA, it followed that the statute cannot be construed to forbid the use or disclosure of credit header information. *See id.* at 37. The court rejected this interpretation of the savings clause and found instead that Congress's decision not to regulate the disclosure of credit header information in the FCRA did not waive Congress's authority to legislate on the subject in the future. *See id.* at 37-38. *Dotzler* concerned a consumer reporting agency's alleged disclosure of address and social security information to a company that was in the business of selling access to public record repositories and proprietary databases. *See* 914 F. Supp. at 329, 330-31. *Dotzler* did not involve voluntary disclosure of this or other credit header information to a government agency.

[redacted]

We believe [redacted]

the FBI is seriously flawed in its failure to explain why the specific limitation on government disclosures in Section 1681f does not control this issue. Therefore, we believe the FBI OGC's adjudication should have addressed the application of Section 1681f before deciding not to report this potential intelligence matter to the IOB. The FBI should reconsider this matter in light of Section 1681f and prevailing case law interpreting this provision. We also recommend that the FBI reconsider its policy and guidance on this issue in light of Section 1681f.[115]

Resolution of this legal question will not only determine whether the potential intelligence violation at issue should be reported to the IOB, but it may also change the results of our judgmental sampling described later in this chapter with respect to the FBI's handling of third party errors. In our judgmental sample, we found that the return data produced to the FBI in response to 13 NSLs requesting limited credit information pursuant to Section 1681u included consumer telephone numbers and, in one instance, date of birth information.[116] If Section 1681f or another statute or regulation prohibits a consumer reporting agency from voluntarily disclosing this information to the FBI, the return data in response to these NSLs should be handled accordingly.

II. The Findings of the FBI Inspection Division's NSL Reviews and the Department's National Security Reviews in 2008 and 2009

In response to the findings and recommendations in the OIG's first and second NSL reports, the FBI and the Department implemented new

---

[115] After reviewing the draft of this report, the FBI restated its determination in the FBI OGC's adjudication memorandum that social security numbers and dates of birth are not protected under the FCRA, and, therefore, it was lawful for the FBI to retain and use this information if the provider voluntarily produced such information to the FBI. However, the FBI stated that it would reconsider this issue.

[116] In our review of Section 1681u NSLs, we found that the FBI frequently included the social security number or date of birth of the NSL target in the letter to the consumer reporting agency to assist the agency in identifying the correct records. In such instances, we did not count the inclusion of the same social security or date of birth information in the return data as an unauthorized collection. However, in the 13 instances we counted as unauthorized collections, the FBI received the telephone numbers and, in one instance, the date of birth of the NSL target in the return data without having provided this information in the letter.

compliance programs that included the periodic inspection of the FBI's use of NSLs. First, the FBI Inspection Division conducted five separate reviews of the FBI's use of NSLs in calendar years 2008, 2009, 2010, 2011, and 2012. The stated objectives of these reviews were to assess the field's compliance with NSL requirements in each calendar year, determine the efficacy of corrective actions taken, and propose additional corrective action, if appropriate.

In addition, in April 2007, the Department implemented a new compliance program for national security investigations. In this program, teams of attorneys from the NSD and the FBI OGC conduct national security reviews in approximately 15-18 field divisions per year. During the period 2007 through 2009, the teams examined a sampling of case files from each office to determine compliance with the requirements for the initiation, extension, and conversion of national security investigations, the issuance of NSLs and the handling of return data, and the reporting of violations to the IOB. During this period, review teams conducted reviews in 42 field divisions (including in 4 field divisions twice) and in the Counterintelligence and Counterterrorism Divisions at FBI Headquarters.

In the sections below, we describe and analyze the key findings made in the FBI Inspection Division's Reports concerning NSLs issued in 2008 and 2009 and in the NSRs conducted in 2007 through 2009. As discussed below, the findings made by the FBI Inspection Division and the NSR teams are generally consistent with the OIG's findings in several respects and confirm that, while certain compliance challenges persist, the FBI's overall compliance with NSL requirements substantially improved in 2008 and 2009.

A. 2008 and 2009 FBI Inspection Division NSL Reviews

1. Methodology

In its 2008 review, the FBI Inspection Division examined 699 NSLs issued between January 1, 2008, and December 1, 2008 ("2008 review"). The NSLs were selected from 15 field divisions and included a random sample of [redacted] percent of subsystem-generated NSLs, as well as all manually generated NSLs issued by those divisions and all NSLs issued by those divisions using another division's investigative file number.[117]

---

[117] This last category of NSLs sometimes occurred when, for example, the FBI's Counterterrorism Division (CTD) sought to issue an NSL for the records of a person who was not an investigative subject of, or otherwise relevant to, an open investigation conducted directly by the CTD at FBI Headquarters. If the person of interest was a subject of or relevant to an open investigation conducted by a field division, the CTD sometimes used the field division's investigative file number to issue the NSL. As discussed later in (Cont'd.)

In its 2009 review, the FBI Inspection Division reviewed 1,560 NSLs issued between December 1, 2008, and December 1, 2009 ("2009 review"). The NSL selection was derived from 16 field divisions and included a random sample of [redacted] percent of subsystem-generated NSLs, as well as review of all manually generated NSLs issued by those divisions and all NSLs issued by those divisions using another division's investigative file number. In addition, the FBI Inspection Division reviewed all FCRA NSLs issued by the divisions covered in its 2009 review, a change from its 2008 review which reviewed FCRA NSLs as part of its random sample only. Most of the NSLs reviewed as part of the 2009 review were issued after December 16, 2008, the effective date of the FBI's DIOG.

2. FBI Inspection Division's Findings

The findings made in the 2008 and 2009 FBI Inspection Division reviews are illustrated in Figures 4.4 and 4.5.

---

this section, the FBI changed its policy on this practice in 2010 in response to the Inspection Division's findings.

FIGURE 4.4
Potential IOB Violations Identified in the 2008 and 2009
FBI Inspection Division NSL Reviews

	2008		2009	
Potential IOB Violation	**Subsystem**	**Manual**	**Subsystem**	**Manual**
NSL issued was not relevant to an authorized investigation	-	-	-	-
NSL issued absent an open preliminary or full national security investigation	-	-	2	-
Voluntary disclosure request issued absent the criteria established in 18 U.S.C. § 2702 (ECPA's emergency voluntary disclosure authority for acquiring non-content information)	-	-	-	-
Investigative file lacked predication or sufficient justification to support the issuance of the NSL	1	-	-	-
NSL lacked approval of an authorized SES official	-	-	-	2
NSL requested information beyond the scope permitted by statute or policy	-	-	-	-
NSL issued with a substantive typographical error in names, addresses, telephone numbers, or the like	1	-	-	-
NSL resulted in receipt of information outside the scope of the NSL request and the additional information was used and/or uploaded into an FBI database	4	-	6	-
TOTALS	**6**	**0**	**8**	**2**

FIGURE 4.5
NSL-Related Compliance Failures Identified in the 2008 and 2009 FBI Inspection Division NSL Reviews as "Administrative Errors"

		2008		2009	
	"ADMINISTRATIVE ERRORS"	***Subsystem***	***Manual***	***Subsystem***	***Manual***
NSL	NSL request did not match EC request	3	28	-	-
	NSL failed to cite the correct statutory authority	1	-	-	-
	NSL failed to identify the specific types of records requested	-	-	-	-
	NSL failed to certify that the information requested was relevant to an authorized investigation	-	-	-	-
Approval EC	EC did not contain a lead for NSLB	-	15	-	12
	EC was not sent to NSLB	-	14	-	15
	EC did not contain a lead for CTD/CD/Cyber	-	10	-	13
	EC was not sent to CTD/CD/Cyber	-	8	-	14
	EC did not indicate transmittal of NSL to squad/field office for delivery	-	5	-	13
	EC failed to list records requested	1	3	-	-
	EC failed to document predication for the NSL	6	2	6	-
	EC failed to document the subject's USPER Status	-	2	-	-
	EC does not have SAC/DAD or above approval	-	1	-	1
	EC failed to identify the type of NSL requested	-	1	-	-
	EC failed to document the justification for the non-disclosure provision contained in the NSL	-	-	1	-
	EC failed to document relevance of the records requested	n/a	n/a	15	-
	EC did not have CDC/ADC or NSLB attorney approval	n/a	n/a	-	-
	EC failed to explain the risk that could potentially arise from disclosure of the NSL	n/a	n/a	3	-
	TOTALS	11	89	25	68

As shown in Figures 4.4 and 4.5 above, the FBI Inspection Division evaluated each NSL on 12 elements, 8 pertaining to potential IOB violations and 4 pertaining to failures to comply with FBI policy, which the FBI classified as "administrative errors." As further shown in Figure 4.5, the FBI Inspection Division also evaluated each subsystem-generated approval EC on 6 elements and each manually generated approval EC on 11 elements, all of which were classified as "administrative errors."

The 2009 review evaluated the NSLs using the same elements as the 2008 review. In addition, the later review included three new "administrative error" categories for both subsystem and manually generated approval ECs: (1) the EC failed to document the relevance of the records requested; (2) the EC did not have CDC/ADC or NSLB attorney approval (legal review); and (3) the EC failed to explain the risk that could potentially arise from disclosure of the NSL.

The FBI inspectors found only 6 potential IOB violations in 699 NSLs issued in 2008 and 10 potential IOB violations in 1,560 NSLs in 2009, which the reports determined yielded 0.9 percent and 0.7 percent PIOB rates, respectively. The reports took the inverse of these two rates to conclude that the reviews revealed a 99.1 and 99.3 percent compliance rate under the law, respectively. Further, the FBI Inspection Division's 2008 Report found a 95 percent improvement in the rate of potential IOB (PIOB) violations by comparing the 0.9 percent PIOB rate in 2008 to the 9.43 percent PIOB rate found in the FBI's 2007 field review of 2003-2006 NSLs.[118] The 2008 Report gave most or all of the credit for this improvement to the FBI's implementation of the NSL subsystem. Similarly, the FBI Inspection Division's 2009 Report credited the NSL subsystem with further reducing the FBI's potential IOB violation rate to 0.7 percent in 2009.

In the 2008 review, the FBI inspectors identified only 11 errors in the 589 subsystem-generated NSLs and the corresponding approval ECs they examined. During an interview with the OIG, the team leader for the 2008 review revised the total number of errors to nine. The team leader told us that, upon further review, two of the errors – one described as "NSL request did not match EC request" and one described as "NSL failed to cite the

---

[118] As described in our second NSL report, in 2007, the FBI Inspection Division conducted a review of 6,688 NSLs issued by the FBI in 2003 through 2006. From this sample, the FBI's inspectors identified 640 potential IOB violations arising from the FBI's use of 634 NSLs, resulting in a PIOB rate of 9.43 percent. This review confirmed that the types of deficiencies identified in our first NSL report had occurred throughout the FBI from 2003 through 2006 and in greater numbers than we had found in our first NSL review, which examined a smaller sample. NSL II Report, 75-100.

correct statutory authority" – were mistakenly identified as errors. Six of the nine remaining errors were failures to document predication in the approval EC.

Although the number of errors found in the 2009 review increased to 25, the 2009 review examined a much larger sample (1,560 NSLs and corresponding ECs), and almost the entire increase can be attributed to the addition of the new error category for failure to document relevance. FBI policy required then, as it does now, that the "four corners" of an approval EC provide a sufficiently detailed explanation of the predication for the investigation and the relevance of the records sought so that NSL approvers have the ability to conduct a meaningful review. It also required that the approval EC document the justification supporting the non-disclosure certification in the NSL when the non-disclosure provision was invoked. Fifteen of the 25 errors (60 percent) identified in the 2009 review concerned the failure to document the relevance of the records requested. The remaining errors consisted of failures to document predication and failures to document the risk of NSL disclosure or the justification for the non-disclosure provision.

As the figure above illustrates, the FBI inspectors found significantly more compliance failures resulting from the use of manually generated NSLs than from the use of NSLs generated by the NSL subsystem, despite the fact that manually generated NSLs and approval ECs comprised a relatively small portion of the 2008 and 2009 sample selections. In 2008, 28 of 32 compliance failures found in NSLs (87.5 percent) and 61 of 68 compliance failures found in approval ECs (89.7 percent) resulted from the use of manually generated NSLs. In 2009, the inspectors found no compliance failures in NSLs – manually generated or subsystem generated – but found that 68 of 93 compliance failures in approval ECs (73 percent) resulted from the use of manually generated NSLs.

With respect to third party errors, the 2008 and 2009 FBI Inspection Division reports found that the FBI appropriately identified and handled overcollections in 94 and 91 percent of all instances, respectively. As illustrated in Figure 4.6 below, in calculating these compliance rates, the FBI reviews focused exclusively on whether the FBI compounded the third party error by using or uploading the additional information, resulting in a potential IOB violation. With respect to uncompounded third party errors, the FBI Inspection Division's reports did not describe the extent to which case agents identified and sequestered overcollections and either redacted, returned, or destroyed any unauthorized information.

FIGURE 4.6
Compliance Rate on FBI Handling of Third Party Errors in 2008 and 2009 FBI Inspection Division NSL Reviews

Third Party Errors	2008	2009
Total # of NSLs	66	65
Potential IOB violation (compounded)	4	6
No potential IOB violation (uncompounded)	62	59
Compliance rate	**62/66 = 94%**	**59/65 = 91%**

3. FBI Inspection Division's Recommendations

In addition to the specific potential IOB violations and compliance failures described above, the FBI Inspection Division reports identified other compliance issues and recommended corrective actions. We discuss the key issues and recommendations below and describe the actions the FBI has since taken to address them.

a. Status of Return Data

In the 2008 review, the FBI inspectors found that case agents did not consistently identify in the NSL subsystem the status of return data, that is, whether the data was received and whether it was reviewed for overcollection. This made return data difficult to track.

The NSL subsystem will send an e-mail notification to the case agent if after 30 days from the date an NSL is issued the case agent has not entered the status of the return data in the subsystem as "received." Shortly before the FBI Inspection Division issued its 2008 report, the FBI upgraded the NSL subsystem to include e-mail notifications alerting supervisors to the absence of entries in the subsystem reflecting the receipt of return data. As a result of this upgrade, SSAs receive notifications of the absence of such entries after 45 days, ASACs after 60 days, and the SAC after 90 days.

To further assist compliance, the FBI Inspection Division recommended in its 2008 report that the FBI upgrade the NSL subsystem to require a specific answer as to whether the return data matched the material requested in the NSL. In response, the FBI OGC upgraded the subsystem to require case agents to check a box next to a field described as "Reviewed for overproduction" on the return information screen page in the subsystem. This check box had existed in the NSL subsystem, but it was

not a mandatory field until this upgrade by the FBI OGC. After the upgrade, an NSL remains in "outstanding" status when this box is unchecked, subject to the escalating e-mail notifications described above that are sent from the subsystem to the case agent and, absent completion, to the case agent's supervisors up to the SAC.

Although the NSL subsystem now includes a mandatory "Reviewed for overproduction" field, it does not require an answer to the more specific question of whether the return data matched the information requested in the NSL or whether the data contained an overcollection. We believe that the FBI should consider implementing this FBI Inspection Division recommendation to encourage greater care and accountability during return data reviews.

b. NSLs Issued Using Another Division's Case File Number

In the 2008 and 2009 reviews, the FBI inspectors identified recurring issues with respect to NSLs issued using another division's case file number.

In its 2008 report, the FBI Inspection Division found that in instances where a division issued an NSL using another division's file number, the auditors had difficulty locating a signed copy of the NSL and a copy of the return data. The records were not consistently maintained by the issuing division, requiring auditors to retrieve the records from the other division's files. Based on this finding, the FBI Inspection Division's report recommended that the FBI OGC instruct field divisions to maintain a copy of the signed NSL and return data generated by their offices using another division's file.

The FBI chose not to implement this recommendation, relying instead on the requirement that signed NSLs and return data be maintained in an NSL sub-file in the substantive investigative file that was used to predicate the NSL. Similarly, the revised DIOG does not include additional requirements for NSLs issued on behalf of other offices. It requires generally that a copy of the signed NSL be retained in the investigative file and that the employee who initiated the NSL request make sure that the return data is maintained in the "appropriate" investigative file.

In its 2009 report, the FBI Inspection Division noted that the 2009 review revealed instances in which the field division responsible for the investigative file (office of origin) was not notified and was unaware that its investigative file was used to issue an NSL. The FBI Inspection Division stated that as a result a signed copy of the NSL and a copy of the return data were not included in the substantive investigative file, as required by

the DIOG. The FBI Inspection Division's report recommended that the FBI update the NSL subsystem so that it automatically notifies the office of origin when another division issues an NSL using its case file number. At that time, the subsystem provided automatic notifications when one field division used another field division's case file number but not when a Headquarters component used a field division case file number. In response to the 2009 review, the FBI upgraded the NSL subsystem to follow the same notification process when a Headquarters component issues the NSL.

To address the record-keeping failures, the FBI Inspection Division recommended in its 2009 review that the CTD designate a centralized component to "track" NSLs and return data. The FBI Inspection Division repeated this recommendation in its report describing its 2010 NSL review, which found failures on the part of the CTD to send copies of signed NSLs and return data to the office of origin's substantive investigative file.[119]

The 2010 NSL review also found that one of CTD's components – the Telephonic Communications Analysis Unit (TCAU) – notified offices of origin of the receipt of NSL return data and advised them to review return data for overcollecton after TCAU had already uploaded the data into FBI databases.[120] The 2010 FBI Inspection Division's Report described this practice as a "serious protocol and policy issue" and recommended that TCAU refrain from uploading NSL return data until an overcollection review is completed and no overcollection is found.[121]

In response to these issues, CTD issued formal guidance in an electronic communication dated December 21, 2010. This guidance emphasized that CTD will not issue NSLs using field division investigative files for routine matters and that when CTD employees issue NSLs using a field division's investigative file they must follow the procedures set forth in the DIOG. The guidance states that CTD employees are responsible for

---

[119] The 2010 NSL review examined NSLs issued between January 1, 2010, and June 30, 2010, before the FBI had an opportunity to implement the improvements recommended in the 2009 NSL review. It is our understanding that NSLs issued in December 2009 were not included in either review.

[120] The Telephonic Communications Analysis Unit (TCAU) is one of the operational support units of the Exploitation Threat Section (XTS) in CTD. Until September 2012, the TCAU was known as the Communications Analysis Unit (CAU) and, until July 2012, the XTS was known as the Communications Exploitations Section (CXS). In July 2012, the FBI reorganized CXS, and, as part of this reorganization, renamed the CXS the Exploitation Threat Section and the CAU the Telephonic Communications Analysis Unit.

[121] As described in more detail in the next chapter, [redacted]. After TCAU serves an NSL and receives the NSL results from the provider, TCAU uploads the NSL results into three FBI databases that store telephone call data.

making "all reasonable efforts" to provide the assigned field division's case agent with signed copies of NSL documents and any material produced in response to an NSL. It further states that the assigned case agent is responsible for reviewing the NSL return data for overcollection.

CTD issued the December 21, 2010, procedures in lieu of designating a centralized component to facilitate appropriate records retention. During an interview with the OIG, an intelligence analyst on CTD's executive staff told us that because more than one CTD component can issue an NSL, the thinking evolved towards procedures that emphasize DIOG requirements instead of a centralized record-keeping strategy.

On June 7, 2012, CTD superseded the December 21, 2010, procedures with new formal guidance that incorporated changes to NSL procedures set forth in the revised DIOG. The new guidance creates separate procedures for NSLs issued from field division's case files and those issued from CTD case files.

The new procedures for NSLs issued from field division's case files are similar to the previous procedures with three key changes. First, the new procedures emphasize that CTD will issue an NSL from a field division's case file only in "exceptional circumstances" and with the concurrence of the Deputy Assistant Director. Second, the new procedures place responsibility for the overcollection review on the CTD employee issuing the NSL, rather than the assigned case agent, to comport with the revised DIOG's requirement that the employee who initiated the NSL request perform the review. Third, the new procedures include a compliance mechanism that requires the CTD employee who issued the NSL to review the return data within 15 days of receipt and draft an electronic communication for the case file that documents, among other things, the records received, whether an overcollection was identified, and to what database the results were uploaded. The EC includes a lead to CTD's executive staff to perform a compliance review.

The new procedures for NSLs issued from CTD case files are substantially similar to the new procedures described above, except that the NSL-related documents must be maintained in the appropriate CTD case file. In addition, the new procedures set forth the circumstances under which CTD may issue an NSL from a CTD case file and require concurrence from the Deputy Assistant Director for all such instances. The procedures prohibit the issuance from CTD case files of NSLs regarding subjects for which a field division already has a predicated investigation.

c. Manually Generated NSLs

The FBI inspectors also identified compliance issues with the processing and tracking of manually generated NSLs. In its 2008 review, the FBI inspectors found that three manually generated NSLs did not meet a valid exception to the mandatory subsystem requirement.[122] The review also found that the FBI lacked a standard approval process for generating NSLs outside the NSL subsystem, as demonstrated by the fact that the FBI Inspection Division required data from three sources – NSLB, the FISA Management Unit, and field divisions – to obtain a complete accounting of the number of manually generated NSLs. The 2008 FBI Inspection Division report recommended that FBI OGC develop a standard process for approving the use of manually generated NSLs and a mechanism to adequately track and monitor manually generated NSLs.

In December 2008, shortly after the period covered by the 2008 review, the FBI issued the first edition of the DIOG, which incorporated specific procedures for manually generated NSLs. This edition of the DIOG provided [redacted] to the mandatory subsystem requirement: [redacted]. The DIOG required agents to use the model NSLs and ECs available on the NSLB website for manually generated NSLs. These model documents prompt case agents to include the same information prompted by the NSL subsystem, including leads to NSLB for congressional reporting purposes and to the relevant Headquarters operational units for informational purposes. In addition, the DIOG required [redacted] generated outside the NSL subsystem.

In the 2009 review, the FBI inspectors found improvement in the FBI's reliance upon the subsystem exceptions. The inspectors found that for each of the [redacted] NSLs generated outside the NSL subsystem during the period

---

[122] According to the 2008 Inspection Division report, the valid exceptions to the mandatory subsystem requirement during the period covered by the review were matters deemed [redacted].

under review, the initiators of the NSL appropriately relied on an exception to the mandatory use of the subsystem. Nevertheless, the inspectors found that field personnel failed to report [redacted] out of [redacted] ([redacted] percent) of the manually generated NSLs to NSLB for congressional reporting. The FBI Inspection Division's report recommended that FBI OGC reinforce training and guidance to ensure that divisions provide NSLB with the information necessary for tracking purposes and congressional reporting.

To improve notification to NSLB of manually generated NSLs, the revised DIOG provides an e-mail address for reporting such matters to NSLB. The revised DIOG also clarifies the circumstances under which prior approval from NSLB is required and requires that the electronic communication authorizing the NSL provide the reason the NSL was generated outside the NSL subsystem and indicate from whom approval was obtained.[123]

The FBI Inspection Division's most recent NSL reviews suggest that the measures the FBI has taken have improved compliance with the requirement to notify NSLB of manually generated NSLs. In its review of NSLs issued between July 1, 2010, and December 31, 2011 ("2010-2011 review"), the FBI inspectors found that field personnel properly reported [redacted] out of [redacted] (96.5 percent) manually generated NSLs to NSLB for congressional reporting. In its review of NSLs issued between January 1, 2012, and December 31, 2012 ("2012 review"), the FBI inspectors found that field personnel properly reported all [redacted] manually generated NSLs to the NSLB for congressional reporting.

However, the most recent NSL reviews identified other issues concerning the FBI's processing and tracking of manually generated NSLs. In the 2010-2011 review, FBI inspectors found that of the [redacted] manually generated NSLs properly reported to NSLB, the NSLB failed to "express" [redacted] of them into the NSL subsystem for congressional reporting purposes.[124] The failure to express the manually generated NSLs into the subsystem means that the NSL data generated by the subsystem for the Department's congressional reports would not have included those NSLs. The FBI Inspection Division recommended that the FBI OGC take steps to ensure

---

[123] In addition, the revised DIOG [redacted].

[124] As described in footnote 72, after the NSLB receives a lead from the field that notifies NSLB of a manually generated NSL, the NSLB's FISA Unit enters the data points for the NSL that are necessary for congressional reporting into the NSL subsystem. The FISA Unit refers to this process as the "expression" of manually generated NSLs into the NSL subsystem.

that all manually generated NSLs reported to the NSLB are expressed into the NSL subsystem.

In the 2012 review, although the FBI Inspection Division did not identify any failures to express manually generated NSLs into the NSL subsystem, the inspectors found that in some cases the NSL subsystem did not accurately reflect the calendar year in which the manually generated NSL was issued. This problem, which can cause errors in congressional reporting, resulted when the NSLB expressed the NSL data into the subsystem before or after the NSL was served, and the date assigned to the NSL by the subsystem reflected a different calendar year than the date in which the NSL was served. The FBI Inspection Division recommended that the FBI OGC take steps to ensure that it accurately tracks the dates of manually generated NSLs.

In response to the FBI Inspection Division's recommendations, the FBI OGC now provides additional information and instruction to the field during the approval process of a manually generated NSL. Specifically, when the NSLB sends an e-mail notification to the issuing office approving the generation of an NSL outside the NSL subsystem, the notification template now requires that NSLB provide the issuing office with the FISAMS ID number assigned by the NSL subsystem to the manually generated NSL. Because a manually generated NSL must be expressed into the subsystem in order for the subsystem to assign a FISAMS ID number, the inclusion of the FISAMS ID number in the notification to the issuing office should help ensure that NSLB expresses the NSL into the subsystem. In addition, the notification template provides an instruction to the issuing office that the NSL should be served within the calendar year reflected in the FISAMS ID number or the office should contact NSLB so that NSLB can assign a new FISAMS ID number reflecting the correct year the NSL is served. The FBI expects that this enhanced notification will help ensure that manually generated NSLs approved by NSLB are properly recorded for tracking purposes. Further, an FBI Inspection Division Section Chief informed the OIG that future NSL reviews will continue to monitor the tracking of manually generated NSLs.

d. FCRAu Unauthorized Collections

In the 2009 review, the FBI inspectors found that while FCRAu NSLs accounted for 46 percent of the total number of NSLs reviewed, they generated almost 59 percent of the third party errors and half of the potential IOB violations identified during the review. Most of these unauthorized collections were caused by one consumer reporting company that provided dates of birth and social security numbers in response to NSL requests for limited credit information under FCRAu.

In its 2009 report, the FBI Inspection Division recommended that the FBI OGC develop specific guidance and training regarding FCRA NSLs and contact the provider to address its production of dates of birth and social security numbers. In response to the FBI Inspection Division's recommendations, the FBI OGC disseminated its *NSL Collection Chart* to all field divisions that identified the categories of information that the FBI OGC believed fell within the scope of the relevant NSL statutes, including the FCRA, and the categories that do not. The FBI OGC also contacted the provider to address the overcollection issue and later sampled return data to make sure that the provider stopped producing dates of birth and social security numbers in response to FCRAu NSLs.

However, the FBI has since changed its policy with respect to the handling of dates of birth and social security numbers in response to NSL requests under FCRAu. As discussed above in Section I.E., the FBI OGC decided not to report a potential intelligence violation to the IOB that involved the receipt of a target's date of birth and telephone number in response to an NSL requesting limited credit information under FCRAu. When the OIG requested clarification of the FBI's policy on this issue, FBI officials told us that the FBI OGC reconsidered the issue in August 2010. According to the FBI, the FBI OGC had not fully analyzed this issue until August 2010, and before then had advised FBI personnel in "an abundance of caution" to treat the additional information as an unauthorized collection. In late September 2010, the FBI OGC determined that social security numbers and dates of birth, "among other information," are not protected from disclosure under the FCRA and that therefore it is lawful for the FBI to retain and use this information if a provider voluntarily produces the information to the FBI. Accordingly, the FBI issued guidance in October 2010 stating that the FBI may retain and use this information to the extent the information is relevant to the investigation.

For the reasons previously described in Section I.E. of this chapter, we believe the FBI should reconsider its change in policy and practice regarding the handling of dates of birth, social security numbers, and telephone numbers received in response to NSL requests under FCRAu. Reconsideration of this issue should include whether Section 1681f of the FCRA prevents consumer reporting agencies from voluntarily providing dates of birth, social security numbers, and telephone numbers to the FBI.

4. OIG Analysis

The FBI inspectors generally found greater compliance with NSL requirements in 2008 and 2009 as compared to the findings made in past NSL reviews, with entire categories of past errors eliminated completely or almost completely as a result of the implementation of the NSL subsystem. The reviews also provided considerable value in terms of highlighting

recurring compliance issues and making recommendations that the FBI OGC and CTD took appropriate steps to address.

At the same time, we believe that the FBI Inspection Division reports may have overstated the extent of the FBI's improvement. As described above, the FBI Inspection Division's 2008 report noted a 95 percent improvement in the rate of potential IOB violations by comparing the 0.9 percent PIOB rate found in the FBI's 2008 review to the 9.43 percent PIOB rate found in the FBI's 2007 review. However, we do not believe the 2007 9.43 percent PIOB rate provides a reliable baseline upon which to measure improvement in the FBI's compliance with NSL authorities. Because of the change in IOB policy described above, the FBI included uncompounded third party errors in the calculation of the 2007 PIOB rate but excluded those errors from the PIOB rate calculations in its 2008 and 2009 reviews. Thus, the reduction in the rate of noncompliance reflected in the FBI's 2008 data resulted in part from a change in the policy that eliminated a category of intelligence violations that previously was reported. Moreover, we concluded in our second NSL review that the FBI 2007 field review did not identify all of the NSL-related potential IOB violations in the case files the inspectors reviewed, which suggested that the actual rate of potential violations for that year would have been somewhat higher.[125] Taking these factors together, we believe the PIOB rates found in the FBI Inspection Division's 2008 and 2009 reviews represent an improvement from the FBI's 2007 field review, but the 9.43 PIOB rate does not provide a reliable baseline upon which to measure the extent of the FBI's improvement.

In addition, with respect to the compliance failures that the FBI Inspection Division's reports categorized as "administrative errors," we believe the FBI omitted two important categories: record-keeping and the FBI's handling of records received as the result of uncompounded third party errors. The FBI Inspection Division's reports did not measure the extent to which the inspectors found hard copies of the necessary NSL-related documents in the appropriate NSL sub-file. Nor did they describe the extent to which case agents identified and sequestered, and redacted, returned, or destroyed, information received as the result of an uncompounded third party error. Instead, the reports based their conclusions regarding the FBI's handling of NSL return data solely on whether or not the FBI compounded the overcollections through the use or uploading of the additional information into FBI databases. In doing so, we believe the reports omitted important data points in evaluating the FBI's compliance with NSL requirements and overstated the FBI's compliance rates on the handling of NSL return data in 2008 and 2009. We recommend

---

[125] NSL II Report, 75-100.

that the FBI incorporate these data points into future FBI Inspection Division reviews of the FBI's NSL use.

Our final observation in this area concerns the FBI's continued characterization of various compliance failures as "administrative errors." Many of these matters involved violations of internal controls designed to ensure appropriate supervisory and legal review of the use of NSL authorities. As we noted in our first and second NSL reports, adherence to these internal controls is necessary to ensure that the FBI's NSL authorities are used appropriately and to facilitate appropriate supervisory and legal review of NSLs.[126] By labeling these compliance failures as "administrative errors," the FBI diminishes their seriousness and fosters a perception that compliance with FBI policies governing the FBI's use of its NSL authorities is annoying paperwork. As we noted in our second NSL report, we discussed this issue with senior FBI officials during the course of our review, and they agreed that the administrative error label could send the wrong message regarding the seriousness of violations of statutes, guidelines, or policies governing the use of NSLs.[127] These officials agreed to consider using a different label, such as "lapses in internal controls," to describe these types of deficiencies. The 2008 and 2009 FBI Inspection Division's Reports, however, continued to use the "administrative error" label, which we believe continues to undermine the seriousness of the violations.

B. 2007-2009 National Security Reviews

In this section, we describe and analyze the key NSL-related findings made in NSRs between 2007 through 2009. During this time period, the Department completed 48 NSRs covering 42 FBI field divisions (4 divisions were reviewed twice due to the number of errors found during the first review) and 2 Headquarters components. In addition to analyzing the written reports documenting these reviews, the OIG interviewed attorneys in the NSD who oversee the NSR program.

1. NSR Methodology

NSR teams are generally composed of attorneys from the NSD and the FBI OGC. Each team also includes, as a source of field expertise, an SSA from a field division other than the one under review. The members of the team change with each review.

---

[126] NSL I Report, 103-107; NSL II Report, 100.

[127] NSL II Report, 100.

The teams conduct reviews in each of the FBI's field divisions approximately once every three or four years. If a review of a particular division reveals a high volume of errors, the program will conduct a follow-up review in that division the following year.

During each field visit, the team reviews a sampling of case files from counterterrorism, counterintelligence, and foreign computer intrusion cyber investigations. The number of case files sampled in each field division varied significantly between 2007 and 2009. In 2007, the number of case files varied between 16 and 45. In 2008, the NSR program standardized the sample size for each NSR to review or attempt to review. The sample size became 35 case files for each small- or medium-size field division and 50 case files for each large field division.

During the reviews conducted between 2007 and 2009 of two FBI Headquarters components, the review teams did not review case files. The teams conducted interviews of personnel in the FBI's Counterintelligence and Counterterrorism Divisions to understand the role of FBI Headquarters in the processing and approval of national security investigations.

The date ranges of the NSLs examined during field visits varied between 2007 and 2009. Many of the early NSRs examined NSLs issued between January 2006 and the date of the review, and every NSL in each of the selected case files was reviewed. The later NSRs generally reviewed NSLs issued between January 2009 and the date of the review. After October 2009, the review teams limited the number of NSLs examined to three per case file.[128]

The review teams examined each case file to determine the FBI's compliance with the Constitution, applicable statutes, the Attorney General Guidelines, and FBI policies in the initiation, extension, and conversion of national security investigations, the issuance of NSLs and the handling of return data, and the reporting of violations to the IOB.[129] Most relevant to

---

[128] The NSD attorney responsible for overseeing the NSR program told us that the NSR teams initially examined every NSL in the case file to understand the types and frequency of compliance issues that arise from NSL use. He told us that this protocol led to the review of a substantial number of NSLs and gave NSD a strong understanding of the issues. Accordingly, by October 2009, the NSD decided to limit the NSL sampling per case file to three.

[129] According to an NSD representative, under current procedures, the NSR review teams no longer examine whether the FBI previously reported potential violations to the IOB or whether every extension to preliminary investigation authority occurred within the 6-month requirement in the Attorney General's Guidelines. According to an NSD representative, the NSD revised the scope of the NSR program to shift the focus from compliance with what the NSD believes are procedural or administrative matters toward compliance with the substantive requirements in the Attorney General's Guidelines.

NSLs, the reviews examined each case file to determine: (1) whether sufficient predication existed to support the investigation; (2) whether there were any lapses in investigative authority; and (3) whether NSLs, the supporting approval ECs, and the handling of return data met NSL requirements. Although NSD periodically revised the specific NSL-related criteria evaluated by the NSR program between April 2007 and December 2009, as a general matter, the requirements were the same or similar to the requirements we evaluated in our past and current NSL reviews.[130]

2. National Security Review Findings

The findings of the first NSRs conducted in 2007 are generally consistent with the OIG's findings in our first and second NSL reviews. Specifically, the NSR reports illustrated widespread errors in the creation of NSLs and approval ECs, the handling of NSL return data, and the retention of records. The findings included:

- NSL or approval EC contained incorrect or no reference to predicate statutory authority;
- NSL and approval EC contained inconsistencies regarding the records requested or the predicate statutory authority;
- NSL or approval EC contained internal inconsistencies regarding the records requested or the predicate statutory authority;
- NSL contained incorrect or lacked certifications required by the predicate statutory authority;
- NSLs and approval EC failed to specify date range for the records requested;
- Approval EC lacked information regarding the U.S. person status of the subject of the investigation or target of the NSL;
- Approval EC did not reflect the required approvals or legal review;
- Approval EC did not provide justification for the invocation of the non-disclosure provisions;
- Approval EC failed to explain the relevance of the records sought to the investigation, including the relevance of requests for [redacted] or calling circle information;

[130] The NSD created the first data collection instrument for the NSR program using several sources as a guide but primarily the data collection instrument the OIG used during the first NSL review.

- Approval EC did not set the required leads;
- NSL issued during a lapse in investigative authority;
- NSL contained typographical mistakes including the transposition of digits in the telephone number, leading to the receipt of records not authorized or not relevant to the investigation;
- FBI obtained information that it either did not request or requested but was not entitled to receive, and provided "little documentation" of the overcollections or the disposition of the overcollections; and
- NSL-related documents were missing from the case file.

The findings in the later NSRs, which generally focused on NSLs issued after the implementation of the NSL subsystem, show an obvious decline in the numbers and categories of NSL-related errors.[131] For example, the later reviews found no instances where approval ECs failed to send required leads to NSLB, the substantive Headquarters component, or the division or squad responsible for serving the letter. More substantively, the later reviews found no instances of NSLs issued during a lapse in investigative authority or approval ECs failing to reflect required approvals or legal review. Moreover, the later reviews showed that although instances of missing, inaccurate, or inconsistent information in the NSLs and approval ECs were not completely eliminated after the implementation of the NSL subsystem, they became increasingly uncommon. The reduction in these errors is significant because, as described throughout this report, such errors in the approval EC can deprive the SAC and other NSL approvers of information needed to knowledgeably authorize the NSL, and such errors in the NSL itself can affect the lawfulness of the NSL request.

To the extent the later NSRs found compliance issues in approval ECs or NSLs, it appears that these issues occurred as a result of data entry errors by case agents responsible for generating NSLs or approval ECs in the NSL subsystem. For example, three post-subsystem NSRs found at least one approval EC that incorrectly identified the U.S. person status of the target. Case agents are responsible for entering U.S. person status in the subsystem workflow. Similarly, in one of the same reviews, the NSR

[131] The 2007 through 2009 NSRs did not report statistics on the NSL-related errors for comparison between different reviews. The NSR reports also did not identify the date of the NSL associated with each error or indicate whether the NSL in question was generated manually or by using the NSL subsystem. Nevertheless, the NSRs conducted after April 2008, which generally focused on NSLs issued between January 1, 2008, and the date of the review, document substantially fewer errors than those documented in NSRs before April 2008.

team found an inconsistency between the description of the records requested in an NSL and the description of the records in the corresponding approval EC's narrative describing the predication for the investigation and relevance of the records requested. The telephone records sought were described correctly in the narrative, but due to a substantive typographical error in the telephone number entered into another portion of the NSL subsystem, the NSL itself identified the wrong telephone number. Consequently, the NSL sought information that was not relevant to the investigation, resulting in a violation of law that required a report to the IOB.

During his interview with the OIG, the NSD attorney responsible for overseeing the NSR program told us that he observed a reduction in NSL-related errors between 2007 and 2009. He attributed most of the reduction in errors to the policy and guidance in the DIOG and the FBI's implementation of the NSL subsystem. With respect to the latter, the attorney told us that the subsystem is a "fantastic" compliance tool and a "great success" for the FBI. He said that he has observed the subsystem reduce the so-called "administrative errors" to "close to zero" and that this improvement has enabled the NSR program to shift its focus to two main issues: whether the approval EC explained the nexus or relevance of the records sought to the investigation and whether any unauthorized collections were identified and handled appropriately.

With respect to these two issues, the NSRs in 2008 and 2009 continued to find failures. For example, the NSRs found many instances where the approval EC failed to explain the relevance or "nexus" of the records sought to the investigation. The NSD attorney told us that sometimes the narrative in the approval EC omitted a discussion of nexus altogether and other times did not sufficiently explain it. The NSR reports also described instances where the narrative did not explicitly identify the telephone number or e-mail account with respect to which records were being sought. According to the NSR reports, these errors typically reflected the failure to document relevant information in the approval EC rather than the absence of relevance as a substantive matter. Nevertheless, as described in the NSR reports, providing a sufficiently detailed explanation of the relevance of the records sought is necessary so that the authorizing officials can make an informed decision about whether to authorize the NSL request. Accordingly, the reports recommended that authorizing officials ensure that approval ECs clearly articulate the nexus between the records sought and the investigation.

Perhaps the most common compliance failure identified in the 2008 and 2009 NSRs was the failure of case agents to identify unauthorized collections and sequester the information in question with the CDC. Nearly all of the post-subsystem NSRs documented at least 1 such failure and a

few documented 10 or more. The failure to identify the unauthorized collections resulted in the retention of unauthorized information in the FBI case file, and, in some cases, the uploading of the information into FBI databases.

Another compliance failure identified in the 2008 and 2009 NSRs was the failure to maintain NSL-related documents in the case file. The NSR teams found that a signed copy of the NSL or a copy of the return data was sometimes missing from one or more case files and unavailable for review.

3. Other Issues Identified in National Security Reviews

In addition to the case-specific findings described above, certain NSRs between 2007 and 2009 raised broader policy issues related to NSLs. We describe the principal issues below.

a. Disposition of Overcollections

Many early NSRs found that the FBI's guidance had been unclear regarding the "disposition" of overcollections. Those NSRs stated an expectation that the guidance contained in the 2007 Comprehensive NSL Guidance EC concerning the identification and handling of overcollections would prevent continuing problems. As an additional measure, the NSRs recommended that NSD work with the FBI OGC to formulate guidance that would address the documentation of the disposition of overcollections and, more specifically, the requirement that the documentation reflect: (1) a description of the information in question; (2) whether the information had been sequestered with the CDC; (3) whether the information had been uploaded and what steps had been taken to sequester such information thereafter; (4) the disposition of any adjudication of the matter by OGC; and (5) the destruction or other disposition of the information and verification that all such information had been removed from FBI electronic files and databases.

In December 2008, the FBI provided additional guidance in the DIOG concerning the handling of overcollections, which largely incorporated the guidance in the 2007 Comprehensive NSL Guidance EC. In addition, in the April 22, 2009, IOB Policy, the FBI provided specific content requirements for reports to the FBI OGC of potential IOB violations and uncompounded third-party errors, which include documentation of any corrective measures taken. Further, to improve uniformity and completeness in the reporting of these matters, the FBI developed the IOB subsystem, which as described elsewhere in this report guides FBI employees through each element of the reporting process.

b. Toll Billing Records

Many early NSR teams found that service providers often provided personal information not enumerated in ECPA Section 2709(b)(1) in response to NSLs requesting "subscriber information and toll billing records." Under Section 2709(b)(1), the FBI may request a person's name, address, length of service, and local and long distance toll billing records. Early NSR reports questioned whether the FBI may legally obtain information about a subscriber that is not specifically enumerated in Section 2709(b)(1), such as social security numbers and dates of birth. The NSRs also questioned whether the types of records listed in the FBI's form attachment to ECPA NSLs seeking toll billing records are within the scope of the phrase "toll billing records" under the ECPA. The FBI took the position then, as it does now, that the FBI cannot legally obtain personal information such as dates of birth and social security numbers in response to NSLs requesting only subscriber information, but can legally obtain such information in response to a request for "toll billing records" if the provider maintained the information as part of its toll billing record in the ordinary course of business.

"Toll billing records" is not defined in the ECPA. In our first NSL review, we reported that service providers produced different types of information in response to the FBI's requests for toll billing records, and that FBI case agents and attorneys had questions about the types of information they can obtain when making requests under this authority.[132] We recommended that the FBI consider seeking a legislative amendment to the ECPA to define the phrase. In response to the OIG's recommendation, and at the FBI's request, the Department drafted a proposed amendment to clarify the phrase, "toll billing records" in the statute.[133] The proposed amendment was sent to Congress on July 13, 2007, and, as of the date of this report, Congress has taken no action on the amendment.

As described in the next chapter, we confronted questions in this review regarding the scope of the term "toll billing records" in Section 2709, and recommend that the Department revive its effort to bring about a legislative amendment to Section 2709 that defines the phrase "toll billing records." We also recommend in the next chapter that during the pendency

---

[132] NSL I Report, 112-113.

[133] The proposed amendment would authorize the FBI to obtain name, address, local and long distance connection records (or session times and durations), length and types of service, telephone or instrument number (or other subscriber number or identity, including any temporarily assigned network address), means and source of payment (including credit card or bank account number), and records identifying the origin, routing, or destination of electronic communications.

of this legislative effort, the Department seek a legal opinion from the OLC on whether information currently requested and received by the FBI through NSLs falls within the scope of the ECPA NSL statute.

4. OIG Analysis

The NSRs conducted in 2007 through 2009 found that the FBI achieved greater compliance with NSL requirements in 2008 and 2009 as compared to 2007 and earlier. The compliance issues that the NSRs identified in 2008 and 2009 concerned failures to explain the relevance of the records requested in the NSL to the investigation, failures to identify and remedy unauthorized collections, and failures to maintain NSL-related documents in the appropriate file.

III. OIG Review

A. Methodology of the OIG Review

As an additional measure of the FBI's compliance with NSL authorities, we conducted a judgmental sampling of 46 counterterrorism, counterintelligence, and cyber case files from two FBI field divisions, Boston and San Francisco.[134] We reviewed up to 5 NSLs in each investigative file, for a total of 165 national security letters issued between January 1, 2008, and December 31, 2009. Of the 165 NSLs in our review, 162 NSLs were generated using the NSL subsystem and 3 were generated manually outside the subsystem.[135]

We selected our judgmental sample using spreadsheets provided by the FBI itemizing each NSL request issued in 2008 and 2009. Based upon this information, we determined that the Boston and San Francisco Field Divisions issued a total of [redacted] NSLs from [redacted] case files. In selecting the 165 NSLs for our review from the 46 case files, we sought to obtain a sampling that would be representative of the NSLs issued by the FBI in 2008 and 2009. We selected NSLs issued from the three types of investigations from which NSLs are issued – counterterrorism, counterintelligence, and foreign computer intrusion cyber investigations. In addition, we made selections that would be representative of the four NSL statutes the FBI routinely relies upon – ECPA, RFPA, FCRAv and FCRAu.

---

[134] A judgmental sampling is a non-probability sampling technique that the OIG has used throughout its NSL reviews to identify potential compliance problems and other issues relevant to the FBI's use of NSL authorities.

[135] The FBI indicated that the [redacted].

Finally, we selected all three manually generated NSLs issued by the Boston and San Francisco Field Divisions to determine whether they differed in any respect from the NSLs generated using the NSL subsystem.

In addition to reviewing the NSLs themselves, we reviewed documentation pertaining to case initiations and investigation authorizations, the approval ECs authorizing each NSL, the recipients' production of documents and electronic media in response to the letters, and any documentation relating to any overcollection or potential IOB violations arising from the NSLs. We also reviewed the entries made in the NSL subsystem for each NSL and, when necessary, interviewed the assigned case agents to obtain additional information about the NSL or investigation. We also interviewed case agents, field supervisors, ASACs, and the SACs in Boston and San Francisco generally about their use of NSLs and NSL-derived information.

B. Failures to Comply with NSL Requirements

1. Potential IOB Violation Identified by the OIG

As described earlier in this chapter, the most serious NSL-related compliance failures are those that result in potential intelligence violations that must be reported to the IOB. In our sample review of investigative files, we found one potential IOB violation arising from the FBI's use of an NSL. This potential violation had not been previously reported to the FBI OGC.

The potential IOB violation identified by the OIG concerned an NSL requesting financial records from a banking institution on July 6, 2009, in connection with a counterterrorism investigation. The NSL request sought the financial records of the subject of the investigation for the 10 and one-half year period of January 1, 1999, to July 6, 2009. The FBI classified the investigation as a sensitive investigative matter under the Attorney General's Guidelines because the subject had an "academic nexus" and the investigation focused on the subject's activities at an academic institution.[136]

136 [redacted]

The approval EC authorizing the NSL request did not articulate the basis for the date range of the request, and the basis for seeking over 10 years of records was not evident from our review of the predicating documents in the investigative file. The case agent who generated the NSL told the OIG that he did not know the reason why the NSL requested over 10 years worth of records. He said there was "no reason" for seeking the subject's financial records as far back as January 1, 1999. Accordingly, because the NSL appeared to seek information not relevant to an authorized investigation, we concluded that this request should have been reported to the FBI OGC for adjudication as a potential IOB matter.[137]

2. NSL-Related Compliance Failures

In addition to evaluating whether any of the NSLs we reviewed may have resulted in a violation of law or Attorney General Guidelines, we examined whether they complied with NSL requirements set forth in FBI internal policies and procedures. The principal policies covering our review period are contained in the original DIOG issued on December 16, 2008, and the Comprehensive NSL Guidance EC issued on June 1, 2007. With few modifications, the DIOG provisions largely incorporated the NSL requirements of the Comprehensive NSL Guidance EC.

We examined whether the NSLs met the following requirements:

- approval EC identified the records requested;
- approval EC stated the type of records requested;
- approval EC indicated the target's U.S. person status;
- approval EC articulated the predication for the investigation;
- approval EC articulated the relevance or nexus between the records sought and the investigation;
- approval EC articulated the justification for the invocation of the non-disclosure provisions;
- approval EC contained the appropriate leads;
- approval EC indicated approval by the necessary approvers;

---

[137] After reviewing the draft of the report, the FBI told the OIG that, according to the issuing field division, [redacted] However, we found unremarkable the determination to seek the target's financial records and raise a question only concerning the basis for seeking over 10 years of records, which the FBI has not explained.

- NSL stated the records requested;
- NSL contained the certification required by the relevant statute;
- the signed NSL, approval EC, and return data were found in the NSL sub-file; and
- any unauthorized information found in the return data was identified and the appropriate corrective actions taken.

We identified 98 compliance failures that violated the NSL requirements described above but did not meet the criteria for IOB reporting. These failures were associated with 65 NSLs from 30 of the 46 case files we reviewed.

FIGURE 4.7
NSL-Related Compliance Failures Identified in the OIG Sample Review of National Security Letters Issued from January 2008 through December 2009

Nature of NSL Compliance Failure	Number of Failures
Approval EC Failed to Identify Records Requested	-
Approval EC Failed to State Type of Records	-
Approval EC Failed to Indicate U.S. Person Status	-
Approval EC Failed to Document Predication	5
Approval EC Failed to Document Relevance or Nexus	4
Approval EC Failed to Document Non-disclosure Justification	1
Approval EC Failed to Contain Leads	-
Approval EC Missing Necessary Approvals	-
NSL Failed to State Records Requested	-
NSL Failed to Contain Required Certification	-
Signed NSL not Found in NSL Sub-file	35
Approval EC not Found in NSL Sub-file	14
Return Data not Found in NSL Sub-file	24
Failure to Identify Unauthorized Collection and Take Corrective Actions	15
Total	**98**

a. Failures to Document Predication, Relevance, and Justification for Non-Disclosure

We found compliance failures in 10 of the 129 approval ECs we examined that related to the case agent's failure to adequately or appropriately document the predication for the investigation, the relevance of the records sought to the investigation, or the justification for the invocation of the non-disclosure provisions.[138] We did not find any compliance failures in the following categories pertaining to the approval

[138] These 10 approval ECs served as the basis for approving 13 separate NSL requests. Further, one of the approval ECs and its corresponding NSL request were manually generated outside the subsystem. The compliance failure associated with this manually generated approval EC – failure to explain the justification for invocation of the non-disclosure provisions – was the only compliance failure we identified in the three manually generated NSLs in our sample review.

EC: failure to state the type of records requested, failure to indicate U.S. person status, failure to specify the required leads, and failure to reflect one or more of the required approvals by authorized officials.

During the period covered by our review, FBI policy required that the "four corners" of an approval EC provide a sufficiently detailed explanation of the predication for the investigation and the relevance of the records sought so that NSL approvers have the ability to conduct a meaningful review. It also required that the approval EC explain the justification supporting the non-disclosure certification in the NSL when the non-disclosure provision was invoked.

Nine of the 10 failures to document predication, relevance, and the need for non-disclosure we found related to the sufficiency of the explanation in the approval EC, rather than the absence of those elements in the case file. By reviewing other documents in the case file and, in one instance, interviewing the case agent assigned to the matter, we were able to verify that sufficient predication for the investigation existed, that the records requested were relevant to the investigation, or that sufficient justification existed for the invocation of the non-disclosure provisions. Accordingly, we categorized these compliance failures as violations of FBI policy, rather than as potential IOB violations. These failures are nevertheless significant because the approval EC forms the basis for the review and approval of the NSL by the squad supervisor, division counsel, ASAC, and ultimately the SAC. Failure to provide sufficient information in the approval EC deprives the individuals in the approval chain from making a fully informed decision about whether or not to approve the NSL.

However, as described earlier in this section, in one instance, we were unable to verify that the records requested were relevant to the investigation and concluded that the matter should have been reported to the FBI OGC for adjudication as a potential IOB matter.[139] In that matter, the approval EC authorizing the NSL request did not articulate the basis for the date range of the request, and the basis for seeking over 10 years of records was not evident from our review of the predicating documents in the investigative file or from our interview with the case agent. Accordingly, because the NSL appeared to seek information not relevant to an authorized investigation, we concluded that this request should have been reported as a potential IOB matter.

---

[139] *See* Section III.B.1, above.

b. Failures to Identify and Remedy Unauthorized Collections Caused By Third Party Error

We reviewed the return data received by the FBI in response to 154 NSLs and, of that number, identified an unauthorized collection in 19 returns.[140] All of these unauthorized collections were caused by third party error. We found that FBI personnel properly identified and remedied 4 of the 19 unauthorized collections upon receipt. Two of these four involved the receipt of records pertaining to an individual or account unrelated to the target, and the other two involved the receipt of records outside the date range requested in the NSL.

We found that 15 of the 19 unauthorized collections, or 79 percent, had not been identified and remedied by the FBI upon receipt, as required by FBI policy, or at any time before our review. None of these unauthorized collections appear to have been compounded by the FBI. Nevertheless, the failure to identify, sequester, and either redact, destroy, or return the unauthorized collection violated FBI policy and resulted in the FBI's retention of information it was not authorized to seek.

Five of these unauthorized collections involved the receipt of [redacted] from one provider in response to NSLs requesting electronic communication transactional records. Specifically, the unauthorized collections included transactional records containing the [redacted]. In each of these five matters, the [redacted]

The NSLs in these five matters did not specifically request [redacted]. However, the provision of [redacted] is not permitted under the ECPA because that statute does not authorize the use of an NSL to obtain the content of an electronic communication. Under 18 U.S.C. § 2510(8), "content" is defined as "any information concerning the substance, purport, or meaning of a communication." Just as subject lines may reveal the content of a communication, so too may the [redacted].

[140] Of the 165 NSLs reviewed by the OIG, 2 NSLs had not been served, and 2 NSLs resulted in no records or written response from the provider. The return data received in response to another seven NSLs was not in the case file and could not be located, which we found troubling. As a result, there were only 154 returns available for our review.

Given that the provider is one of the larger e-mail service providers, we would expect that the FBI received [redacted] from this provider in response to many more NSLs requesting electronic communication transactional records.[141] We are not aware of this issue having been identified or brought to the attention of the FBI OGC before our review, and we do not believe any guidance had been given to the field before our review regarding whether [redacted] may be received in response to an NSL. It is therefore likely that unauthorized information of this type remains undetected in other FBI case files.

After we identified this issue during our review, [redacted][142]

Four other unauthorized collections involved the receipt of information other than name, address, and length of service in response to subscriber-only ECPA NSLs, such as date of birth, payment-related information, and service plan or features. Two additional unauthorized collections involved the inclusion of records unrelated to the targeted name or account in an otherwise responsive production. One other involved the receipt of financial institution information in response to a FCRAu NSL that requested consumer-identifying information only.

The remaining unauthorized collections concerned the receipt of [redacted] from one provider in response to three NSLs requesting toll billing records in 2008 and 2009. In each instance, the provider produced an Excel spreadsheet that revealed the [redacted], although the NSLs did not request this information. [redacted] is not among the types of information the FBI can request pursuant to the NSL statutes.[143] A San Francisco Field Division

---

[141] According to the FBI OGC, the FBI issued [redacted] NSLs to this provider requesting electronic communication transactional records since January 1, 2008.

[142] The redactions in this paragraph are of information the FBI identified as classified and privileged attorney-client communications.

[143] The government is generally required to seek an order from the FISA Court to obtain this information, or, in a criminal investigation, a court order under 18 U.S.C. § 2703(d) or a probable cause search warrant under 18 U.S.C. § 2703(c). [redacted]

(Cont'd.)

official told the OIG that the provider did not stop producing this type of this information in response to NSLs until sometime in 2011, which suggests that there are likely many more examples of this type of unauthorized collection in the FBI's case files.[144]

During our interviews with case agents and supervisors assigned to counterterrorism and counterintelligence squads in Boston and San Francisco, we asked them about their experiences with handling unauthorized collections. We found that the case agents and supervisors appeared to be mindful of the need to review return data to make sure that providers produce records for the requested target and within the requested date range. This raised the question of why then had the field divisions we visited failed to identify 15 of 19, or almost 80 percent, of the unauthorized collections we found in our review.

Taking into consideration the types of unauthorized collections we found and information provided in our interviews, we concluded that case agents may not be as mindful or even aware of the types of unauthorized collections that are less obvious than those involving the wrong target or date range. All four unauthorized collections identified during our review that FBI personnel had identified and remedied upon receipt included records for the wrong individual or phone number, or accounts or records outside the requested date range. By comparison, 13 of the 15 unauthorized collections the FBI had not identified consisted of NSL return data for the correct target and the correct date range but included information beyond the scope of the relevant NSL statute, such as: [redacted]; subscriber information other than name, address, and length of service; and financial institution information in response to a FCRA NSL seeking consumer-identifying information only. This suggests that case agents may not have given enough attention to the scope of the information permitted under the NSL statutes when conducting their reviews of NSL return data.

Many of the case agents and supervisors we interviewed said that they either did not use, did not recall whether they ever received, or were

[redacted]

[144] According to the FBI OGC, the FBI issued [redacted] NSLs to this provider requesting toll billing records since January 1, 2008.

generally not aware of reference material or other guidance to assist them in making unauthorized collection determinations, such as the *NSL Collection Chart* the FBI OGC disseminated to field divisions in late 2010. Most of these case agents and supervisors told us that such guidance would or could be helpful to them in making these determinations. Two told us, however, that such guidance would be of limited or no value because the identification of unauthorized collections is "simple" or "pretty obvious," which further supports our conclusion that some agents and supervisors may conduct an unduly simplified review of NSL return data that can result in missed unauthorized collections.

c. Record-keeping Failures

Seventy-three of the 98 compliance failures we found in this review concerned the FBI's failure to maintain NSL-related documents in the appropriate case files.

In our first NSL review, we found that the FBI did not routinely retain copies of signed NSLs, rendering impossible a comprehensive audit of the FBI's compliance with its internal control policies and the statutory certification requirements for NSLs.[145] In response to that finding, the FBI required in June 2007 that a copy of every signed NSL and the responsive return data be maintained in the investigative file. The FBI later incorporated these requirements into the DIOG. To further assist future audits, the FBI required beginning on March 20, 2008, that all signed NSLs, approval ECs, and records produced in response to an NSL be maintained in a "National Security Letter" sub-file in the investigative file.

In this review, we found that 1 or more NSL-related documents were missing from the NSL sub-files in 24 of the 46 case files we reviewed, or in 52 percent of the files. As noted, while we did not conduct a statistically significant random sampling, the high rate of deficient record-keeping we found in our judgmental sampling strongly suggests that this problem is not uncommon.

We found that 15 NSL sub-files lacked signed copies of 30 NSLs. The FBI found signed copies of 2 of these 30 NSLs in other files. However, the FBI was unable to produce to the OIG signed copies of the remaining 28 NSLs. As a result, we were unable to verify that an authorized official had signed these 28 NSLs.

We also found that four sub-files contained signed copies of five NSLs that the providers had included along with their return information. We

---

[145] NSL I Report, 107, 125.

found no other copies of the signed NSLs in these sub-files. We concluded that the presence of the provider copies in the files did not demonstrate compliance with the FBI's record-keeping requirements. The FBI's policy requires that a copy of every signed NSL and the responsive return data be maintained in the investigative file. Although the availability of the provider copies in these few instances made it possible to verify that an authorized official had signed the NSLs, the FBI cannot guarantee this result in every case because it does not control whether a third party provider returns a copy of the signed NSL with the provider's response to the NSL. Therefore, it is important that case agents ensure that a copy of the signed NSL is placed in the file upon issuance.

With respect to other NSL-related documents, we found that the relevant NSL sub-files lacked 14 approval ECs, one of which was ultimately found in another file. The field divisions accessed electronic versions of the remaining 13 approval ECs using the ACS database, or its successor Sentinel, and printed copies for our review. With respect to NSL return data, we found that the relevant NSL sub-files lacked the return data provided in response to 24 NSLs. The returns for 17 of these 24 NSLs were found in another file. The remaining seven were never located and, therefore, were unavailable for inspection during our compliance review.

d. Additional Observation Concerning Record-keeping

During our review, we found that the NSL subsystem reflected the status of the return data as "outstanding" for two of the three manually generated NSLs we reviewed in our sample even though the field division had received the return data. We therefore requested clarification from the FBI as to whether it had a policy or practice requiring the use of the NSL subsystem to record and track the status of NSL return data for manually generated NSLs. In response, the FBI told us that the requirement in the DIOG that case agents document the receipt of return data in the NSL subsystem applies to all NSLs, however they are generated. However, the DIOG does not state the requirement in this manner, and we believe an explicit policy or guidance is warranted to help ensure that case agents understand their responsibility to make these entries in the NSL subsystem for manually generated NSLs after such NSLs are entered into the subsystem. We recommend that the FBI clarify its policy and guidance on this issue. We also recommend that the FBI consider an upgrade to the NSL subsystem that would prompt case agents to record the same entries in the NSL subsystem for the return data of manually generated NSLs as are required for subsystem generated NSLs and send escalating e-mail notifications when they have not done so. If implemented, this upgrade should help ensure that the FBI has an adequate tracking mechanism for the return data of all NSLs, however they are generated.

C. OIG Analysis

In this review, we examined a judgmental sample of 165 NSLs issued by two FBI field divisions between January 1, 2008, through December 31, 2009, in connection with 46 counterterrorism, counterintelligence, and cyber case files. We examined each NSL and related documents to evaluate the FBI's compliance with NSL requirements set forth in the NSL statutes, Attorney General Guidelines, and the FBI's internal policies and found greater compliance with NSL requirements in this review than we had found in our previous NSL reviews.

We first examined whether any of the compliance failures identified in our judgmental sample required that the FBI report the matter to the IOB under the then-existing reporting criteria because the matter involved an error that may have been unlawful or contrary to Executive Order or presidential directive, or because the matter was a "significant or highly sensitive matter," whether or not unlawful or contrary to Executive Order or presidential directive. In our sample review, we found only one potential IOB violation arising from the FBI's use of an NSL. This potential violation, which had not been previously reported to the FBI OGC, arose from the FBI's request for financial records pursuant to the RFPA NSL statute for a longer time period than appeared from the documentation and our interview with the case agent to be relevant to the investigation. We concluded that this request should have been reported to the FBI OGC for adjudication as a potential IOB matter for seeking information not relevant to an authorized investigation.

By comparison, in our first NSL review, we identified 22 potential IOB violations in a larger judgmental sample review of 293 NSLs issued from 4 field divisions between 2003 through 2005.[146] More than half of the potential violations we identified (12 of 22) resulted from FBI errors in the issuance of the NSL. One FBI error was a field division's issuance of an NSL after authorization for the underlying investigation expired. The other 11 resulted from NSL requests lacking the approval of the SAC, seeking content under the ECPA, citing the wrong NSL statute as authority for the request, omitting the certification language required by the applicable NSL statute, and requesting a full credit report in a counterintelligence case. We found none of these FBI errors in the current review.

The remaining 10 potential IOB violations found in our first NSL review involved unauthorized collections caused by third party error. At least one of these unauthorized collections was uploaded into an FBI database. Even assuming the other 9 matters involving unauthorized

---

[146] NSL I Report, 79-83.

collections were removed based on the change in the FBI's IOB reporting policy (discussed above), 13 potential IOB violations would remain from the total of 22 potential IOB violations we found in NSL I.

In our second NSL review, we identified 15 potential IOB violations in a judgmental sample of 169 NSLs issued by 3 FBI field divisions between 2003 through 2006.[147] Four of the potential violations resulted from FBI error and 11 resulted from initial third party error. The four FBI errors included substantive typographical mistakes in the names, addresses, or telephone numbers targeted in the NSL, and NSL requests lacking the necessary predication or justification. We found no FBI errors in this review caused by a substantive typographical mistake and only one error caused by a request lacking the necessary predication or justification.

The remaining 11 potential IOB violations found in our second NSL review involved unauthorized collections caused by third party error. It is unknown how many of these unauthorized collections the FBI compounded through the use or uploading of the unauthorized information because, as discussed above, the FBI's IOB policy regarding the reporting of uncompounded third party errors did not change until April 2009, after the period of our second NSL review. Even if all 11 of these potential violations were removed based on the change in the FBI's IOB policy (discussed above), 4 potential IOB violations would remain from the total of 15 potential IOB violations we found in our second NSL review.

As compared to the findings of our previous NSL reviews, the finding of only one potential IOB violation in our current review suggests improvement in the FBI's compliance with the NSL statutes in 2008 and 2009.

We also examined in this review whether the FBI complied with NSL requirements set forth in its internal policies and procedures. In total, we found 98 compliance failures that violated FBI policy or procedure but did not meet the criteria for IOB reporting. These failures were associated with 65 NSLs from 30 of the 46 case files we reviewed and fell into 1 of 3 categories: (1) failure to include required information in the approval EC; (2) failure to identify and remedy uncompounded unauthorized collections caused by third party error; and (3) failure to maintain NSL-related documents in the appropriate case files. We identified 10 failures in the first category, 15 failures in the second, and 73 in the third. One of the failures in the first category was associated with one of the three manually generated NSLs in our sample. We found no compliance failures in the national security letters themselves, all of which, whether subsystem or

[147] NSL II Report, 93-100.

manually generated, included the information required by the applicable NSL statute.

By comparison, in our first NSL review, we identified 155 violations of FBI policy or procedure in our sample review of 293 NSLs issued between 2003 through 2005. These compliance failures were associated with 46 of 77 case files and fell into 3 categories: (1) failure to document review of approval EC by one or more required supervisors or division counsel; (2) failure to include required information in the approval EC; and (3) failure to include required information in the national security letter. We found 32 failures in the first category, 123 failures in the second, and 5 failures in the third. We also identified 66 approval ECs that did not include required transmittals either to FBI Headquarters operating divisions or field divisions responsible for service of the NSL.[148]

When comparing these results to the results of our current review, three aspects of our first NSL review should be considered. The first is that the judgmental sample in our first NSL review was almost twice as large as the judgmental sample in this review - 293 NSLs as compared to 165. The second is that the 155 compliance failures we identified in the first NSL review did not include the FBI's failures to identify and remedy unauthorized collections that were caused by third party error and not compounded by the FBI through use or uploading of unauthorized information. At the time of the first review, those failures were considered potential IOB violations, rather than violations of FBI policy. Finally, the 155 compliance failures did not include any failures to maintain NSL-related documents in the appropriate case files. The FBI did not require that copies of all signed NSLs, approval ECs, and records produced in response to NSLs be maintained in a "National Security Letter" sub-file in the investigative file until March 2008, in response to the repeated record-keeping problems we identified in our first and second NSL reviews. Accordingly, the current review is our first review of the FBI's compliance with these new record-keeping requirements.

Nevertheless, a comparison of the results in this review to the results of our first NSL review is informative in four important areas. As shown in Figure 4.7, this review revealed: (1) no failures to document necessary approvals in the approval EC, as compared to 32 in the first review; (2) 10 failures to include required information in the approval EC, as compared to 123 in the first review; (3) no failures to include required information in the

[148] NSL I Report, 104-07. In our second NSL review, we did not independently review FBI case files for violations of FBI policy and procedures. Instead, we reviewed and analyzed the findings of the FBI's 2007 field review and focused our own judgmental sample review on an assessment of the 2007 FBI field review's identification of potential IOB violations.

national security letter, as compared to 5 in the first review; and (4) no failures to include required transmittals in the approval EC, as compared to 66 in the first review. We therefore concluded that, similar to the results of the FBI and the Department's internal reviews, the results of our review suggest that the FBI's compliance with its policies and procedures generally improved in 2008 and 2009.

However, as in the internal reviews, we identified compliance challenges in the FBI's use of NSLs in 2008 and 2009. First, we found that although the FBI had better record-keeping policies in 2008 and 2009, a significant number of NSL-related documents were missing from the NSL sub-files we reviewed. Indeed, we found that half of the sub-files we reviewed lacked one or more NSL-related documents. We therefore believe that future training and guidance should re-emphasize the importance of sending NSL-related documents, including NSL return data, to the appropriate NSL sub-file.

Second, we found 15 instances in which case agents failed to identify an unauthorized collection caused by third party error and take the appropriate corrective action. This number represented almost 80 percent of the unauthorized collections we identified in our sampling.

Based on interviews, we found that case agents appeared to be mindful of the need to review return data to make sure that the provider produced requested records on the correct target and within the correct date range. In fact, all four unauthorized collections identified during our review that had been timely identified and remedied by the FBI concerned records of the wrong individual or records outside the requested date range. We found, however, that case agents were not as mindful or even always aware of the less obvious types of unauthorized collections, such as the receipt of financial or service plan information in response to a subscriber-only NSL or the receipt of [redacted] in response to an NSL requesting transactional records. The FBI provided more specific guidance on identifying unauthorized collections in its *NSL Collection Chart,* but not until late 2010. More than half of the case agents we interviewed were not even aware that such guidance existed, indicating that the FBI OGC should do more to publicize the chart and re-emphasize training and guidance in this area.

Further, 5 of the 15 unauthorized collections we found involved the receipt of [redacted] from a large e-mail service provider in response to NSLs requesting electronic communication transactional records, and another 3 involved the receipt of [redacted] from a nationwide cell phone service provider. Because the FBI issued over [redacted] NSLs to these providers since January 1, 2008, collectively, there are likely many more unauthorized collections from these providers in FBI

case files. The FBI OGC represented to the OIG that the process the FBI would need to undertake to identify and remove any additional unauthorized collections from its case files in 56 field divisions and FBI Headquarters would be very labor intensive. We believe the FBI should notify the IOB about the unauthorized collections found in this review containing [redacted] from the two providers and seek guidance on whether the FBI should undertake the effort necessary to identify and remove similar unauthorized collections that likely remain in many FBI case files.

Finally, we found 10 compliance failures in the 129 approval ECs we examined caused by the failure to include required information. These compliance failures were limited to documentation of three requisite categories of information: the predication for the investigation, the relevance of the records requested, and the justification for the invocation of the non-disclosure provisions. These failures are nevertheless significant because the approval EC forms the basis for the review and approval of the NSL by the squad supervisor, division counsel, ASAC, and ultimately the SAC. Failure to provide sufficient supporting documentation in the approval EC deprives the individuals in the approval chain from making a fully informed decision about whether or not to approve the NSL. To help reduce future errors, future training and guidance should re-emphasize the importance of properly establishing these elements in the approval EC and the need for supervisors and legal reviewers to closely scrutinize the narratives provided by case agents.

We make recommendations at the end of this chapter to help the FBI address these compliance challenges.

IV. OIG Conclusions and Recommendations

The results of our review and the reviews conducted by the FBI's Inspection Division and the NSR program revealed similar trends regarding the FBI's compliance with NSL requirements in 2008 and 2009. It appears that the corrective measures taken by the FBI and the Department in response to the findings and recommendations made in the OIG's first and second NSL reports have significantly increased the FBI's compliance with applicable law and policy in its use of NSLs.

We believe that the substantial improvement demonstrated in 2008 and 2009 is largely attributable to the FBI's implementation of the NSL subsystem. The subsystem reduced opportunities for human error by including drop-down menus, limited choices, and self-populated fields. Ordered tasks and automated notifications ensure that each NSL receives the required legal and supervisory review and approval. We believe these

improvements are reflected in the results of our review. We identified no potential IOB violations involving subsystem-generated NSLs that cited the wrong statute, requested full credit reports in counterintelligence matters with no counterterrorism nexus, or lacked the approval of an authorized Senior Executive Service official. We found no instances of NSLs failing to describe the records requested or failing to include the required statutory certification. We also found that approval ECs contained the information necessary for Congressional reporting. The reviews conducted by the FBI's Inspection Division and the NSR program demonstrated similar results.

At the same time, the NSL subsystem cannot eliminate FBI errors completely and must rely upon the careful entry of accurate information. For this reason, we believe the FBI's mandatory training on NSL requirements and IOB reporting and the policies and procedures in the Comprehensive NSL Guidance EC and, later, the DIOG also contributed significantly to the FBI's improved compliance.

In short, the FBI's corrective measures appear to have provided guidance and internal controls on NSL use that did not exist in 2003 through 2006, and these measures have resulted in substantial improvement in the FBI's compliance with NSL requirements.

Nevertheless, the FBI experienced some compliance challenges in 2008 and 2009. We found that the FBI OGC reported 112 NSL-related potential intelligence violations in 34 matters to the IOB for activity that appears to have occurred in 2008 and 2009. Almost a quarter of these violations involved a substantive typographical error in an NSL caused by mistakes in the identification of a telephone number, e-mail address, or social security number for the target of the NSL. These violations demonstrate the importance of careful entry of information into the NSL subsystem. Almost all of the remaining violations involved the FBI's use or uploading of unauthorized information that had been erroneously provided to the FBI.

We found that the greatest compliance challenge for the FBI in 2008 and 2009 was in the identification of unauthorized collections. Even though there are prompts in the system and escalating supervisory reminders to require some level of agent review for overcollection, we found that the FBI had not previously identified and remedied almost 80 percent of the 19 unauthorized collections identified in our sampling. A comparison between this review and our first NSL review revealed that the identification of unauthorized collections was the only category where we found more rather than fewer errors in 2008 and 2009. The reviews conducted by the NSR program demonstrate that this problem was not isolated to the files we reviewed as nearly all of the post-subsystem NSRs documented at least one

unauthorized collection that had not been remedied by the FBI and a few documented 10 or more.

In interviews with the OIG, case agents appeared to be mindful of the need to review return data to determine whether the provider had produced records regarding the correct target and within the correct date range. In fact, all four unauthorized collections found in our review that the FBI had identified and remedied in a timely manner involved records regarding the wrong individual or records outside the requested date range. We found, however, that case agents were not as mindful or even always aware of the less obvious types of unauthorized collections, such as the receipt of financial or service plan information in response to a subscriber NSL or the receipt of [redacted] in response to an NSL for transactional records. In late 2010, the FBI provided additional guidance to help agents identify unauthorized collections in its *NSL Collection Chart*. However, we found that the FBI should do more to publicize the chart as more than half of the case agents we interviewed said they were not aware that such guidance existed, demonstrating the need for greater emphasis on training in this area.

Further, 5 of the 15 unauthorized collections we found in our review involved the receipt of [redacted] from a large e-mail service provider in response to NSLs requesting electronic communication transactional records, and another 3 involved the receipt of [redacted] from a regional cell phone service provider. Because there are likely many more unauthorized collections from these providers in FBI case files, we believe the FBI should notify the IOB concerning the unauthorized collections found in this review containing [redacted] from the two providers and seek guidance on whether the FBI should undertake the effort necessary to identify and remove similar unauthorized collections that likely remain in other FBI case files.

Another significant compliance issue is the lack of sufficient description in approval ECs of the relevance of the records sought in the NSL to the underlying investigation. While 93 percent of the approval ECs we reviewed did not present this issue, the results of our review, the NSRs, and the FBI's 2009 NSL review demonstrate that the failure to explain relevance was the most frequent compliance failure in approval ECs in 2008 and 2009. In December 2009, the FBI made the narrative entry for the relevance description a mandatory field in the NSL subsystem, so that case agents can no longer move to the next step in the NSL process without completing this step. This enhancement to the NSL subsystem may help focus agents' attention on the need to articulate the relevance of the records to the investigation. Future training and guidance should re-emphasize this element of the approval EC.

In our review, we found one or more NSL-related documents missing from the NSL sub-file in more than half of the case files we reviewed. Future training and guidance should also remind case agents to ensure that all NSL-related documents, including return data, are maintained in the NSL sub-file.

Finally, we found significant delays in FBI's adjudication of potential IOB matters. The FBI OGC took an average of 427 days, or about 14 months, to report the 34 matters to the IOB. In the most egregious example, the FBI OGC took 919 days, or about 2 and one half years, to adjudicate a matter involving what appeared to be a relatively straightforward, compounded overcollection. While the IOB subsystem is an improvement in the FBI OGC's management of the IOB reporting process, we believe it will not address the main causes of the FBI OGC's slow pace in reporting potential intelligence violations to the IOB. The FBI should take additional steps to address the substantial delays in adjudication caused by limited resources and competing priorities.

Based on our review, we recommend that the FBI:

1. Provide periodic training and guidance re-emphasizing the importance of: (1) sending NSL-related documents, including NSL return data, to the appropriate NSL sub-file, and (2) properly documenting and scrutinizing the predication for the investigation, the relevance of the specific records requested in the NSL to the investigation, and the justification for the invocation of the non-disclosure provisions in the approval EC.

2. Take steps to ensure that case agents and supervisors assigned to national security investigations are aware of and adhere to FBI OGC guidance pertaining to the identification of information that is beyond the scope of an NSL request, including providing additional training and assuring that the guidance contained in the FBI OGC's *NSL Collection Chart* is well publicized and easily accessible.

3. Notify the President's Intelligence Oversight Board concerning the unauthorized collections found in this review containing [redacted] from two providers and seek guidance on whether the FBI should undertake the effort necessary to identify and remove similar unauthorized collections that likely remain in many FBI case files.

4. Upgrade the NSL subsystem in the FISA Management System to require that case agents verify whether NSL return data matched the information requested in the NSL and whether it contained an overcollection. In addition, consider an upgrade that would require that

case agents make the same entries in the NSL subsystem for the return data of manually generated NSLs as are required for subsystem generated NSLs and send escalating e-mail notifications when those entries are not made.

5. Reconsider whether Section 1681f of the FCRA prohibits a consumer reporting agency from voluntarily providing the FBI with an NSL target's date of birth, social security number, or telephone number in response to a FCRA NSL under Section 1681u, and provide additional guidance as appropriate.

6. Take additional steps to address the substantial delays in the FBI OGC's adjudication of potential IOB matters caused by limited resources and competing priorities.

7. In future compliance reviews conducted by the FBI Inspection Division, incorporate the examination of two additional data points: (1) the extent to which NSL documents are maintained in the appropriate NSL sub-file; and (2) with respect to uncompounded third party errors, whether the FBI took the appropriate remedial measures in conformity with FBI policies and procedures.

CHAPTER FIVE
OTHER NOTEWORTHY ISSUES RELATED TO THE FBI'S USE OF NATIONAL SECURITY LETTERS

In this chapter, we describe other noteworthy issues related to the FBI's use of national security letters that we encountered during our review. These matters include the scope of the term "toll billing records" in Section 2709 of the ECPA and the FBI's policy on the uploading of NSL-derived information into FBI databases after the authorizing investigation has closed or after the authority for the investigation has expired.

I. Telephone Toll Billing Records

As we have noted in this and our previous NSL reports, the ECPA generally prohibits providers of a remote computing service or electronic communication service from disclosing "a record or other information pertaining to a subscriber to or a customer of" their services.[149] As an exception to this general prohibition, ECPA Section 2709 allows the FBI to request, and requires the providers to supply, "the name, address, length of service, and local and long distance toll billing records of a person or entity" upon written certification by the FBI Director or his designee that the records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that any investigation of a U.S. person "is not conducted solely on the basis of activities protected by the first amendment."[150]

The statute does not define "toll billing records," and there is little case law interpreting the statutory phrase. Moreover, the types of records that may be considered "toll billing records" have expanded along with technological developments in the last 25 years. When the ECPA NSL statute was first enacted in 1986, most households had one landline telephone and were billed for local and long distance telephone calls. Now, many individuals have cell phones or disposable cell phones, pre-paid phone cards, fixed-rate phone plans, and text messaging capabilities.

---

[149] 18 U.S.C. § 2702(a)(3).

[150] Section 2709(a) states that a provider shall comply with a request for "subscriber information," "toll billing records information," and "electronic communication transactional records" under Section 2709(b). Section 2709(b)(1) allows the FBI Director or his designee to request "name, address, length of service, and local and long distance toll billing records." Thus, the "toll billing records information" that the FBI may request and that the provider must furnish is limited to "local and long distance toll billing records," also referred to in the statute and in this report as "toll billing records."

In our first NSL report, we found that uncertainty about the meaning of the phrase "toll billing records" had generated confusion both for providers and FBI employees. We therefore recommended that the Department consider seeking a legislative amendment to the ECPA to define the phrase.[151]

Based on a recommendation from the FBI, the Department drafted a proposed amendment to clarify the scope of the FBI's authority under Section 2709. The proposed amendment was cleared by the Office of Management and Budget and sent to Congress on July 13, 2007, but was not enacted. The proposed amendment would have authorized the FBI to obtain the following records in response to ECPA NSLs:

- name;
- address;
- local and long distance telephone connection records, or records of session times and durations;
- length of service (including start date) and types of service utilized;
- telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;
- means and source of payment for such service (including any credit card or bank account number); and
- records identifying the origin, routing, or destination of electronic communications.

In our second NSL report, we stated that, if enacted, the proposed amendment to the ECPA NSL statute would clarify the meaning of the phrase "toll billing records" by specifying the types of records and information that the FBI can obtain in counterterrorism and counterintelligence investigations from electronic communication service providers and remote computing services.[152] As of the date of this report, the ECPA NSL statute remains unchanged.

Against this backdrop, we examined in this review records that the FBI obtained in response to ECPA NSLs in 2008 and 2009. We sought to determine whether the records fell within the scope of information that the FBI may obtain under Section 2709.

---

[151] NSL I Report, 112-113.

[152] NSL II Report, 32-33.

In the course of this review, we identified three issues that we believe warrant further consideration. The first is whether the [redacted] obtained by the FBI through NSLs served by the Telephonic Communications Analysis Unit (TCAU) of the Exploitation Threat Section (XTS) in the Counterterrorism Division at FBI Headquarters fall within the scope of "toll billing records."[153] The second issue is whether the FBI may receive the personal information of a subscriber other than name, address, and length of service in response to NSLs requesting toll billing records. The third is whether the FBI may request and receive toll billing records for all telephone numbers "associated with" the account of a targeted telephone number without first determining and certifying the relevance of those records to an authorized national security investigation.

As described below, with respect to the first and second issues, we conclude that the ECPA NSL statute and existing guidance do not clearly establish whether the information falls within the scope of toll billing records. With respect to the third issue, we believe that the plain language of the ECPA requires the FBI to first determine whether the records of telephone numbers associated with the account of the targeted telephone number are in fact relevant to a national security investigation before seeking such records directly through an NSL.

A. Telephone Records Obtained Through TCAU

In the Exigent Letters Report, we observed that the records provided to the CAU at FBI Headquarters by one telephone carrier, which we referred to as Company A, in response to exigent letters and other informal methods contained features that were not available to FBI agents in the field who served NSL requests on Company A.[154] Because the records Company A provided to the TCAU [redacted], we sought to determine whether the records provided to the TCAU fell within the scope of "toll billing records" under Section 2709.

1. Background

As we described in our first NSL report and our Exigent Letters Report, the TCAU was established in approximately July 2002 as one of four

---

[153] As we describe in Chapter Four, when the FBI first established the TCAU, its name was the Communications Analysis Unit (CAU), and it was one of the operational support units of the Communications Exploitations Section (CXS) in CTD. In July 2012, the FBI reorganized CXS, and, as part of this reorganization, renamed the CXS the Exploitation Threat Section (XTS) and the CAU the Telephonic Communications Analysis Unit (TCAU).

[154] Exigent Letters Report, 50-51.

units created within the XTS to support the FBI's investigative and intelligence mission. The TCAU's specific mission is to exploit terrorist communications and provide actionable intelligence to the CTD. Relevant to this review, the TCAU serves NSLs for toll billing records upon [redacted] and uploads the return information into three FBI databases used for retention and analysis of telephone records.[155]

We interviewed the TCAU personnel who supervise the service of NSLs and manage the three telephone databases where the return information is maintained. Unless otherwise noted, the procedures they described to us have remained substantially the same throughout our review period and continued through at least 2012. According to these witnesses, [redacted]. The TCAU currently serves NSL requests and receives return information from two telephone carriers, Company A and Company C, under separate contracts the FBI maintains with these carriers. Until 2009, the TCAU also served NSL requests and received return information from a third telephone carrier, Company B, under a contract the FBI maintained with Company B.[156]

According to the TCAU personnel we interviewed, the TCAU's role since 2009 with regard to NSLs originating from FBI field divisions begins

---

[155] We described the history and functions of the TCAU in more detail in our first NSL report and our Exigent Letters Report. *See* NSL I Report, 87-99; Exigent Letters Report, 14-25. In those reviews, we reported that between 2003 and 2006 the TCAU improperly obtained ECPA-protected information from three telephone carriers through the use of so-called "exigent letters" and other informal methods without, or in advance of, appropriate legal process. We also reported on the apparent lack of training, guidance, and oversight provided to the TCAU by CTD management, FBI OGC attorneys, and FBI senior leadership, which we concluded contributed to the improper practices in the TCAU. *See* Exigent Letters Report, 217-256. By contrast, in this review, we describe the information obtained by the TCAU through properly issued NSLs.

[156] Company A, Company B, and Company C are the three telephone carriers described in our Exigent Letters Report that provided telephone records to the TCAU in response to exigent letters and other informal requests between 2003 through 2006. As described in our Exigent Letters Report, the FBI entered into contracts with these carriers in 2003 and 2004, which required that the communication service providers place their employees in the TCAU's office space and give these employees access to their companies' databases so they could immediately service FBI requests for telephone records. Exigent Letters Report, 20. As described in the next chapter, the TCAU no longer shares office space with the telephone providers. Companies A and C continue to service FBI requests for telephone records and provide the records electronically to the TCAU. Company B did not renew its contract with the FBI in 2009 and is no longer providing telephone records directly to the TCAU. Company B continues to provide telephone records in response to NSL requests issued directly by the field without TCAU's assistance.

when the field division generates an NSL that seeks toll billing records from one of two telephone carriers, Company A or Company C. After the SAC or other authorized official signs the NSL, field division personnel send the approval EC and the original signed NSL to the TCAU. The approval EC includes a lead requesting TCAU to serve the NSL. TCAU personnel then serve the signed NSL [redacted] and receive the return information from the carrier [redacted].

The special agent in the TCAU who receives the return information performs an overcollection review and sends responsive information to the TCAU Tech Team.[157] The Tech Team prepares the information for uploading into three separate FBI databases and then asks the special agent to verify that the return information is responsive to the NSL request and appropriate for uploading into the databases. At that time, the special agent performs a second overcollection review. Once the Tech Team receives verification that the special agent did not find any unauthorized information, the team uploads the return information into three separate FBI databases. Once the return information is uploaded, the special agent sends the original NSL return information to the original requester in the field.

In the event unauthorized information is identified during the first or second overcollection review, the TCAU special agent confirms the unauthorized collection with the provider, deletes the information from the [redacted], and requests and obtains the responsive records from the provider.

The NSLs that TCAU personnel serve upon Company A and Company C [redacted]. In order to effectuate service by the TCAU, the case agent who generates the NSL in the NSL subsystem must enter the carrier address used by the TCAU and must include a lead in the approval EC requesting that the TCAU serve the letter.[158]

---

[157] As we described in previous chapters, this report uses the term "overcollection" to describe information that is beyond the scope of an NSL request and the term "unauthorized collection" to describe overcollections that contain information that the provider was prohibited by statute to disclose to the FBI ("unauthorized information").

[158] According to the special agent in TCAU who manages the service of NSL requests, [redacted]. He also told us that the TCAU will serve approximately [redacted] legal documents requesting telephone records each week, on average. NSLs constitute more than [redacted] percent (Cont'd.)

Company A and Company C respond to NSL requests served directly by a field division as well as to those served through the TCAU. According to TCAU personnel, [redacted]; and (3) as described below, Company A and Company C [redacted].

2. Telephone Records Obtained by the TCAU in Response to NSLs

Our review showed that providers produced [redacted]. For example, the material [redacted]. *See* Appendix A. [redacted], the material Company A [redacted]. *See* Appendix B.

The [redacted] by Company A in response to NSLs issued by the TCAU included the following information [redacted]:

- records of all [redacted];
- records of [redacted];
- records of [redacted];
- [redacted];
- records showing [redacted];

---

of those requests, with the rest consisting of grand jury subpoenas, administrative subpoenas, and court orders.

- records showing [redacted]; and
- records of [redacted].

The material Company A provides in response to NSLs served by the TCAU [redacted]. For example, [redacted]. TCAU personnel told us that [redacted][159] [redacted].

The return information also contains [redacted]. *See* Appendix C.

Company C provides call records to TCAU [redacted]. *See* Appendix D. By contrast, the call records provided by Company B before its contract with the FBI ended in 2009 [redacted]).

TCAU personnel told us that Company A and Company C [redacted]. TCAU personnel told us that [redacted]

[159] This [redacted], for which, as described in the previous chapter, [redacted].

[redacted] an [redacted].

Significantly, Company A and Company C [redacted]. TCAU personnel we interviewed [redacted]. TCAU personnel told us that [redacted]. Similarly, our review of NSLs showed that [redacted].

3. FBI OGC Guidance

We sought to determine whether the FBI OGC had provided guidance to TCAU personnel concerning whether the records obtained by the TCAU fell within the scope of "toll billing records" as used in ECPA Section 2709. Specifically, on April 27, 2012, we requested that the FBI describe the guidance and oversight provided by the FBI OGC to the TCAU on the scope of information that may be lawfully obtained in response to an NSL seeking telephone toll billing records.

The FBI OGC provided a written response on October 2, 2012 stating that it had not located "any formal written guidance from [the FBI OGC] to [the TCAU] that explicitly reviews [redacted] that was in use during the period of [the OIG's] review and provides an opinion that obtaining those [redacted] is lawful." The response also stated that "we are not able to determine precisely when the [redacted] was determined to fall within the scope of information that may be lawfully obtained by the FBI in response to an NSL seeking toll billing records." According to the FBI, because it did not have a "specific prior written record" of such a determination, NSLB attorneys in the FBI OGC "recently considered the issue" in response to the OIG's request and concluded that the data falls within the scope of information that may lawfully be obtained in response to an ECPA NSL.[160]

[160] We asked the FBI for any documentation reflecting FBI OGC consultation during the contract renewal process for Company A, Company B, and Company C in 2009 and its (Cont'd.)

We also requested that the FBI explain [redacted] Company A and Company C provided to TCAU fell within the scope of "toll billing records." Rather than explain [redacted], the FBI OGC stated that [redacted] that does not pertain to a subscriber or customer and are therefore not protected from disclosure pursuant to ECPA Section 2702(a)(3), and that [redacted] within the meaning of "toll billing records" because the information could be used by the provider to assess a charge to its customer for the calls. In support of this position, the FBI cited a legal opinion issued by the Office of Legal Counsel dated November 5, 2008.

The November 2008 OLC opinion addressed whether the phrase "local and long distance toll billing records" in ECPA Section 2709(b)(1) includes records of incoming and outgoing calls regardless of whether the provider actually assesses a charge for the calls, and regardless of whether the provider maintains such records in subscriber-specific records or in aggregate form. Drawing support from legislative history and descriptions of terms commonly understood by the communications industry, the OLC opinion concluded that any call record that a communications provider keeps in the regular course of business and that could be used for billing a subscriber falls within the scope of Section 2709, regardless of how the information is stored or whether it is used to bill a subscriber. The opinion stated that the statute would not authorize the FBI to seek, or the provider to disclose, any record simply because the provider has already created it in the ordinary course of business. Instead, the opinion stated that the pivotal question is whether the records in the carrier's custody or possession are "usable" or "suitable" for billing purposes.[161]

---

approval of the new contracts with Company A and Company C. On January 30, 2013, the FBI provided the OIG with documents reflecting e-mail communications between personnel in the Counterterrorism Division and the Chiefs of the FBI OGC's Procurement Law Unit and National Security Law Branch regarding the language in the draft statement of work for each renewal contract. The documents tend to show that procurement and subject matter experts within the FBI OGC reviewed and approved the draft statements of work, which identified the [redacted] to be provided in response to NSLs served by the TCAU consistent with our findings set forth above. The documents do not state whether, during this review and approval process in 2009, the FBI OGC reviewed [redacted] identified in the draft statements of work for legal sufficiency and determined that the information fell within the scope of Section 2709.

[161] The OLC opinion drew support from *In re Grand Jury Subpoenas to Southwestern Bell Mobile Systems, Inc.*, 894 F. Supp. 355 (W.D. Mo. 1995), which considered whether a grand jury subpoena for "telephone toll billing records" issued pursuant to Section 2703 of the ECPA allows a grand jury to obtain records of local as well as long distance telephone calls. In what is the only published opinion we have found interpreting the scope of "toll billing records" under the ECPA as of the date of preparation of this report, the United States District Court for the Western District of Missouri held that "telephone toll billing records" as then used in Section 2703 covered all records of calls

(Cont'd.)

We believe that some of the data Company A and Company C provide to the TCAU appears to fall relatively easily within the OLC opinion's definition of toll billing records because the information could be used for billing purposes. For example, [redacted].

However, application of the OLC opinion's definition to other aspects of the data is less straightforward. For example, as described above, Company A and Company C [redacted]. The OLC opinion does not state that "[redacted].

Accordingly, we are unable to conclude that [redacted] falls within the scope of "toll billing records" as used in the ECPA. Our recommendation concerning the specific steps the FBI and the Department should take to clarify the FBI's authority to obtain this information in response to an ECPA NSL is set forth at the end of this chapter.

B. Personal Information Other Than Name, Address, and Length of Service

The second question we encountered regarding the scope of "toll billing records" is whether the term includes certain personal information relating to a subscriber, such as date of birth and social security number. As noted previously, the NSL statute does not expressly permit the FBI to request or a provider to furnish information other than the "name, address, length of service, and local and long distance toll billing records of a person or entity." *See* 18 U.S.C. § 2709(a) and (b). Further, since the term is not defined, it is unclear whether "toll billing records" includes anything other than the records of incoming and outgoing calls.

---

from or attributed to a particular number, regardless of whether, in fact, a separate charge was assessed for each call. *See Southwestern Bell*, 894 F. Supp. at 359. According to the OLC opinion, in 1996 Congress amended the ECPA statute to ratify the decision in the *Southwestern Bell* case by inserting the words "local and long distance" before the words "toll billing records" in both Section 2703 and 2709.

As discussed in Chapter Four, we observed during our review that on occasion telephone carriers provided a social security number or date of birth in response to an NSL request for toll billing records. The NSL letter template the FBI used, and still uses, to request toll billing records does not specifically include the subscriber's date of birth and social security number in its attached list of requested records. Instead, the list requests, among other things, "[s]ubscriber name and [redacted] The list does not define [redacted] or limit the phrase to name, address, and length of service. The internal guidance to FBI personnel, including the *NSL Collection Chart* prepared by the NSLB, provides that dates of birth and social security numbers may be obtained in response to a request for toll billing records if the information is part of the subscriber's billing information and is maintained by the provider as part of the subscriber's toll billing records.

In its November 2008 legal opinion, the OLC stated that in response to a request for toll billing records a "provider can disclose information if it is a 'toll' record of an incoming or outgoing call, as explained above. If the information is not such a 'toll' record, the provider can disclose it only if it is 'subscriber information' – the 'name, address, and length of service' of the subscriber." If, as suggested in the OLC's opinion, a toll record pertains only to an incoming or outgoing call, it follows that a date of birth or social security number is not a toll record, and that information does not fall within the opinion's definition of "subscriber information."

In the written reports of national security reviews in 2007, the NSR review teams repeatedly raised the question whether the FBI is entitled to obtain personal information about a subscriber, such as a date of birth or social security number, in response to an NSL request for toll billing records. The reports noted that the FBI had taken the position that it may not obtain social security numbers and dates of birth in response to an NSL request for subscriber-information only, but that such information could constitute "toll billing records." Raising questions about the FBI's interpretation of the NSL statute, the reports stated:

> This issue is identified here because it is not clear from the language of the statute that the FBI can legally obtain information about a subscriber that is not specifically enumerated in Section 2709(b)(1) ("name, address, length of service"). It is also not clear that the types of records listed in the FBI's attachment to ECPA NSLs seeking toll billing records falls within the scope of the definition of toll billing records under ECPA. On August 28, 2007, FBI OGC requested an opinion from the Office of Legal Counsel regarding certain ECPA issues which was informed by the information disclosed by the March 2007 DOJ IG report on NSLs and the National Security

Reviews undertaken since April 2007. However, this request did not seek guidance on whether the term "toll billing records" encompasses personal information or those items in the FBI's attachment to NSLs requesting toll billing records.

Although the NSR reports questioned the FBI's interpretation of the NSL statute, including whether the records identified in the FBI's attachment to ECPA NSLs fall within the scope of "toll billing records," the FBI did not seek to clarify this issue with the OLC or in the Department's proposed legislative amendment to the ECPA NSL statute.[162] The proposal that cleared the Office of Management and Budget and was sent to Congress on July 13, 2007, did not include social security numbers or dates of birth in its proposed definition of "toll billing records."

[redacted] In addition, the Deputy Assistant Attorney General who manages the Law and Policy Section within NSD told the OIG that NSD lawyers are considering the issue of whether Section 2709, as it currently exists, permits the FBI to obtain personal information of the subscriber other than name, address, and length of service, such as date of birth, social security number, and credit card information, in response to requests for electronic communication transactional records.

The FBI's internal guidance on this issue is similar to its guidance on toll billing records, that is, the FBI may obtain the information to the extent it is maintained as part of the provider's electronic communications transactional records. The Deputy Assistant Attorney General of NSD's Law and Policy Section told us that he expected any conclusions reached by the NSD on this issue to apply equally to toll billing records provided by telephone carriers since those records "parallel" electronic communication transactional records.

In sum, the FBI's authority to request or receive a subscriber's date of birth or social security number as part of a request for "toll billing records" is unclear. Our recommendation concerning the specific steps the FBI and the Department should take to clarify the FBI's authority to obtain this information in response to an ECPA NSL is set forth at the end of this chapter.

---

[162] During our review, we did not observe any changes to the description of records attached to the FBI's ECPA NSLs from 2007 through 2009.

C. "Associated" Telephone Records

The NSL template the FBI uses to request toll billing records includes the following language in its attached list of requested records: [redacted][163] We found during this review that in response to this request telephone carriers have sometimes produced the subscriber information and toll billing records of individuals other than the individual believed by the FBI to be using the telephone number identified in the NSL.

For example, as described in Chapter Four, according to a potential IOB matter reported by one field division to the FBI OGC in April 2008, the field division issued an NSL request for toll billing records of a telephone number the FBI believed was used by the subject of an investigation. The approval EC for the NSL noted that the investigative subject's telephone number was assigned to an account subscribed to by the subject's mother. In response to the NSL request, the FBI received the records of the investigative subject's telephone number as well as three additional sets of toll billing records for telephone numbers not specifically identified in the NSL. Because the telephone number believed to be used by the investigative subject was part of a joint or family plan of telephone numbers subscribed to by the subject's mother, the provider produced the toll billing records for other numbers assigned to the mother's account.

After receipt, the case agent determined that the additional telephone numbers were not known to be associated with the investigative subject and that the additional records were not relevant to the investigation. However, in its written adjudication of this potential IOB matter, the FBI OGC determined that the potential violations were not reportable to the IOB because [redacted] The adjudication memorandum did not expressly state how the FBI OGC reached this determination, but referred to [redacted] The adjudication does not state or reflect that the FBI OGC considered whether the approval EC established the relevance of the "associated" records. We reviewed the approval EC and found that it

---

[163] The FBI's templates for ECPA NSLs seeking electronic communication transactional records or electronic subscriber information include [redacted].

did not address the relevance of the "associated" records or state that the NSL request sought those records.

As illustrated in this example, the significance of the FBI's request for "associated" records is that the FBI has sought and in some cases received not only the toll billing records and subscriber information of the specific telephone number identified in the NSL, but also the toll billing records and subscriber information on any and all additional telephone numbers that belong to the same account – such as numbers in a group or family plan account – without a separate determination and certification by the FBI that the additional records are relevant to an authorized international terrorism investigation. Yet before the FBI may specifically request in an NSL the records of a subject's family member or partner, Section 2709 would require an authorized official to certify that such records are relevant to a national security investigation.

We have found nothing in the ECPA that would permit the FBI to use NSLs to request or receive the telephone toll billing records or electronic communication transactional records of any individual without certifying that those records are relevant to an authorized national security investigation. Instead, we believe that the plain language of the ECPA requires the FBI to first determine whether the records of a family member, business partner, or other individual associated with the account of the telephone number identified in an NSL are in fact relevant to a national security investigation before seeking such records directly through the NSL. In other words, the FBI should not be able to request in an attachment what it would not be able to request in the NSL itself.

This is not the first time questions have been raised about the FBI's authority to seek or receive "associated" records. In our second NSL report, we identified the receipt of telephone toll billing records for the "family plan" of individuals who were not relevant to an authorized investigation as being among the most serious potential IOB violations that had not been previously identified by the FBI.[164]

The OIG expressed similar concerns in the Exigent Letters Report regarding the FBI's practice of requesting [redacted]. The FBI agreed with our finding that this practice was contrary to the requirements of the NSL statute and issued guidance in the DIOG advising

[164] NSL II Report, 97.

that [redacted] could not be sought unless their relevance was established beforehand.

Similarly, we believe that the ECPA requires that the FBI first determine whether the subscriber information and toll billing records of others who may be associated with the targeted account are in fact relevant to a national security investigation before seeking such records directly through an NSL. Our recommendation concerning the steps the FBI should take to ensure that FBI personnel do not request or obtain "associated" records without a separate determination and certification of relevance to an authorized national security investigation is set forth at the end of this chapter.

D. Conclusion

As the foregoing illustrates, the FBI obtains many types of information in response to NSL requests for toll billing records, and it is unclear whether all of them fall within the scope of Section 2709.

First, we observed that the telephone records provided in response to ECPA NSLs requesting toll billing records were [redacted]. We concluded that the ECPA NSL statute does not clearly establish whether [redacted] falls within the scope of toll billing records.

Second, we observed that telephone carriers sometimes provided a social security number or date of birth in response to an NSL request for toll billing records. This information is not specifically enumerated in Section 2709 among the categories of information that the FBI may request or receive using an NSL.

To address these issues, we believe that the Department should revive its effort to bring about a legislative amendment to Section 2709 by submitting another proposal that more precisely defines the phrase "toll billing records." We believe the legislative proposal should clearly specify the categories of telephone and electronic records that the Department seeks to have Congress define as falling within the scope of ECPA Section 2709, in order to ensure that the FBI does not seek or obtain information to which it is not authorized. We believe that in devising any new legislative proposal, the Department should consider whether the [redacted], and consumer identifying information such as dates of birth and social security numbers, should be included among those the Department seeks to have specifically included within the scope of Section 2709. Finally, because a legislative change may take time,

we believe the Department should simultaneously seek a legal opinion from the OLC as to whether the information described in this chapter and in the FBI's template attachment to ECPA NSLs falls within the scope of Section 2709.

The third issue we identified concerned the FBI's practice of requesting and receiving records "associated with" the records targeted in NSL requests. With respect to this issue, we believe that the plain language of the ECPA requires the FBI to first determine whether the records of a family member, business partner, or other individual associated with the account of the telephone number identified in an NSL are in fact relevant to a national security investigation before seeking such records directly through the NSL. The FBI should take steps to ensure that FBI personnel do not request or obtain "associated" records without a separate determination and certification of relevance to an authorized national security investigation.

II. Handling of NSL Return Data Received Post-Investigation

In this review, we observed that the FBI sometimes received the return data from an NSL request after the authorizing investigation had closed or after the authority for the investigation had expired. In the seven such instances we identified, we found that the FBI received, reviewed and, in one instance, uploaded the information into an FBI database.

With respect to the instance in which the FBI uploaded the information into an FBI database, the field division reported the matter to the FBI OGC as a potential IOB violation. The report stated that the FBI issued an NSL request for toll billing records during the authorized investigation and that, after the authority for the investigation expired, the case agent reviewed and analyzed the records received and uploaded them into the FBI's Telephone Applications database. The FBI OGC determined not to report the potential intelligence violation to the IOB. In its adjudication memorandum, the FBI OGC reasoned that [redacted] The FBI OGC based its reasoning on then-controlling Attorney General Guidelines for FBI National Security Investigations (NSIG), [redacted]

Based upon the NSIG and the Attorney General's Guidelines that supersede it, we agree that the FBI may receive and review records that it obtained through a properly issued NSL request after the authorizing

investigation has closed or after the authority for the investigation has expired. Nevertheless, we questioned the FBI OGC's decision to allow FBI personnel to upload the records into FBI databases and retain them without any consideration of the future investigative value of the records balanced against the individual's right to privacy, particularly given that a decision had been made that continuation of the investigation was not warranted. For example, it is not difficult to imagine a scenario in which the FBI may decide to close an investigation based upon evidence that completely exonerated the investigative subject as a threat to the national security, such as evidence establishing mistaken identity. In such instances, we believe the individual's right to privacy may outweigh the potential for future investigative value of the information such that uploading the individual's information into FBI databases that are widely accessible within the FBI and intelligence community would not be justified.

For this reason, we believe the FBI should consider implementing a policy that would require agents, in consultation with OGC attorneys, to carefully balance the privacy interests of the individual against the potential for future investigative value before permitting the uploading into FBI databases of NSL results received after a case has closed or after the authority for the investigation has expired.

III. Recommendations

For the reasons described above, we make the following recommendations to the FBI and the Department:

1. The FBI and the Department should revive their efforts to bring about a legislative amendment to Section 2709 by submitting another proposal that defines the phrase "toll billing records." We believe the legislative proposal should specify the categories of telephone and electronic records the Department seeks to have Congress define as falling within the scope of ECPA Section 2709, in order to ensure that the FBI does not seek or obtain information to which it is not authorized. We believe that in devising any new legislative proposal, the Department should consider whether the [redacted], and consumer identifying information such as dates of birth and social security numbers, should be included among those the Department seeks to have specifically included within the scope of Section 2709. Finally, because a legislative change may take time, we believe the Department should simultaneously seek a legal opinion from the OLC on whether the information described in this chapter and in the FBI's template attachment to ECPA NSLs falls within the scope of Section 2709.

2. The FBI should take steps to ensure that the FBI does not request or obtain "associated" records without a separate determination and certification of relevance to an authorized national security investigation. These steps should include, but not necessarily be limited to, the incorporation of guidance in the Domestic Investigations Operations Guide and in training materials making clear that before seeking "associated" records in an NSL, the relevant FBI officials must make a separate determination and certification that those records are relevant to an authorized national security investigation.

3. The FBI should consider implementing a policy that would require agents, in consultation with OGC attorneys, to carefully balance the privacy interests of the individual against the potential for future investigative value before permitting the uploading into FBI databases of NSL return data received after a case has closed or after the authority for the investigation has expired.

CHAPTER SIX
STATUS OF THE FBI'S AND THE DEPARTMENT'S CORRECTIVE ACTIONS IN RESPONSE TO THE OIG'S EXIGENT LETTERS REPORT

During our first NSL review, we discovered the FBI's practice of issuing "exigent letters," instead of national security letters or other legal process, to obtain telephone records from three electronic communications service providers. These letters requested telephone records based on alleged "exigent circumstances," which in many cases did not exist and inaccurately stated that grand jury subpoenas had already been sought for the records. Although the FBI's inadequate documentation of this practice made it difficult to determine the total number of exigent letters issued, we were able to confirm that the Communications Analysis Unit of the FBI's Communication Exploitation Section (CXS) in the Counterterrorism Division (CTD) issued over 700 exigent letters seeking records between March 2003 and November 2006.[165] The CAU issued the letters to three providers, who placed their employees in FBI office space in order to expedite FBI requests for information. We also found that another 76 exigent letters were issued by the New York Field Office and other field offices and by Headquarters units other than CAU.

We concluded that the use of exigent letters circumvented the requirements of the ECPA and also violated Attorney General Guidelines and FBI internal policy. The exigent letters were signed by CXS personnel who were not authorized to sign NSLs; in some instances there was no pending national security investigation associated with the request at the time the exigent letter was sent; despite representations to the contrary, some letters were used in non-emergency circumstances and were not followed up with legal process; most letters did not limit the records sought by date range; and CAU personnel uploaded the data received in response to the letters without first reviewing the data for unauthorized information.

In our Exigent Letters Report issued in January 2010, we examined the use of exigent letters in depth. The report described how the FBI's practice of using exigent letters evolved, how widespread it became, and the management failures that allowed it to occur. We determined that the FBI's CAU issued at least 722 exigent letters between March 2003 and December

---

[165] As noted in Chapter Five, in July 2012, the FBI reorganized CXS, and, as part of this reorganization, renamed the CXS the Exploitation Threat Section (XTS) and the CAU the Telephonic Communications Analysis Unit (TCAU). The events described in this chapter occurred before the Section and the unit were renamed, so we refer to them here as the CXS and CAU, respectively.

2006 requesting information on more than 2,000 different telephone numbers. In addition, our report identified other informal ways by which the FBI obtained records from on-site providers without legal process, including requests made by e-mail, face-to-face interactions, on post-it notes, and by telephone. We also described the practice referred to by the FBI and the providers as "sneak peaks" where the providers would describe the information contained in their databases to FBI personnel before the issuance of legal process to help the FBI determine whether to seek the records.

We described other improper practices related to telephone records, such as community of interest or calling circle [redacted].

We also described the improper use of administrative subpoenas under 21 U.S.C. § 876 to obtain fugitive location information, requests by grand jury subpoenas and other means for reporters' telephone records in three media leak investigations without the required Attorney General approval, and inaccurate statements made to the FISA Court regarding the source of information contained in certain FISA applications.

After we issued our first NSL report in March 2007, the FBI ended its use of exigent letters and took other corrective actions to address the problems that resulted in and from their use. However, to address the other improper practices uncovered during our in-depth review of exigent letters, we recommended in our Exigent Letters Report that the FBI and the Department take additional action to ensure that FBI personnel comply with the statutes, guidelines, regulations, and policies governing the FBI's authority to request and obtain telephone records.

In a letter dated April 1, 2010, the FBI agreed with 10 of the 13 recommendations made in our Exigent Letters Report and stated that it would implement, and in some instances had already implemented, the recommended reforms. With respect to two recommendations, the FBI either deferred to the Department to respond to the recommendation or stated that it would coordinate implementation with the Department's National Security Division. With respect to one other recommendation, the FBI stated that it would review its policies, without stating whether it agreed with the recommendation.

In a letter dated April 13, 2010, Associate Deputy Attorney General Matthew Olsen responded to four recommendations that were also directed specifically toward the Department. The letter stated that the Department had taken steps toward implementing all four recommendations.

In this chapter, we assess the FBI's and the Department's efforts to implement the recommendations made in our Exigent Letters Report. In Section I, we summarize our previous recommendations and analyze the efforts undertaken to implement them. In Section II, we set forth our conclusions and additional recommendations.

I. Status of the Implementation of the OIG's Recommendations

In this section, we summarize each OIG recommendation and the corresponding FBI response, and then provide the OIG's analysis. Where the FBI has taken specific action on a recommendation that fully addresses the issue(s) the OIG identified, we consider the recommendation "closed." Where the FBI has taken specific action on a recommendation but we request additional action or information to address the issue(s) the OIG identified, we consider the recommendation "resolved" but not yet closed. Upon completion of the requested action or receipt of the requested information, we will consider whether to close the recommendation.

As described below, we conclude that the FBI and the Department have fully implemented 8 of the 13 recommendations, which we consider closed. Four recommendations are resolved but not closed because the FBI or the Department must provide additional information or take additional action before the OIG can determine whether to close the recommendation. One recommendation concerning guidance on hot number [redacted] remains open.

Recommendation 1
Status: Closed

OIG Recommendation: In our Exigent Letters Report, we assessed the accountability of FBI officials and employees for their roles in the use of exigent letters and the other improper practices described in the report.[166] We found that FBI supervisors and attorneys did not take sufficient action to oversee and prevent the use of exigent letters and other improper requests for telephone records. We also found that the performance of some FBI employees who signed the exigent letters that were inaccurate on their face was not in accord with the high standards expected of the FBI and

[166] Exigent Letters Report, 213-256.

other law enforcement personnel. We concluded that officials at every level of the FBI were responsible in some way for the numerous, repeated, and significant failures that led to the FBI's use of exigent letters and other improper requests for records over an extended period of time. Accordingly, we recommended that the FBI assess the information developed in our review to determine whether administrative or other personnel action was appropriate for the individuals involved in the use of exigent letters and other improper requests for telephone records.

FBI Response: After the OIG issued the Exigent Letters Report, the FBI informed the OIG that it had referred individuals involved in the use of exigent letters and other improper practices to the FBI's Office of Professional Responsibility (FBI OPR) for appropriate action. As a result of the referrals, the FBI OPR informed the OIG that it took the following actions between June and December 2010:

- The FBI OPR did not find misconduct with respect to 28 individuals but requested that the individuals receive non-disciplinary counseling regarding their roles in the use of exigent letters and other improper practices or the management failures that contributed to their use.[167]
- The FBI OPR did not find misconduct as to one individual and did not request that the individual receive non-disciplinary counseling.
- The FBI OPR administratively closed the inquiries concerning eight individuals due to these individuals' retirement or resignation.

OIG Analysis: The FBI implemented this recommendation by referring the individuals involved in the use of exigent letters and other improper requests to the FBI OPR for a determination as to whether administrative or other personnel action was appropriate. According to the FBI OPR's written memoranda reflecting its adjudications of the referrals, the FBI OPR made final determinations as to all 36 FBI employees we identified as having had involvement in the use of exigent letters or other improper practices, as well as one other individual. The OIG is closing this recommendation because the FBI has made final determinations regarding whether to take administrative or other personnel action as to each of these individuals.

---

[167] In each of these administrative inquiries, FBI OPR considered whether the employees ran afoul of FBI Offense Code 1.8, which prohibits employees from "[k]nowingly or recklessly failing to enforce or comply with an FBI or DOJ operational guideline or policy not specifically delineated in any of the other 'Investigative Deficiency' offense codes . . ., which falls outside the parameters of performance."

Recommendation 2
Status: Resolved

OIG Recommendation: In the course of our review of the FBI's use of exigent letters, we discovered other informal practices that resulted in the FBI obtaining telephone records without satisfying the requirements of the ECPA and other statutes, Attorney General Guidelines, and FBI policy. To address these additional deficiencies, we recommended that the FBI provide periodic guidance and training regarding applicable authorities, including the ECPA, the Pen Register Act, federal regulations governing subpoenas for toll billing records of reporters, and the FBI's administrative subpoena authorities.[168]

FBI Response: According to the FBI's April 1, 2010, response to the OIG's Exigent Letters Report, the FBI addressed this recommendation in four ways.

First, the response stated that the FBI provided comprehensive guidance regarding the FBI's authority to obtain telephone records in the DIOG, which the FBI issued in December 2008 and revised in October 2011. The DIOG contains guidance on each investigative technique available to obtain ECPA-protected information. This guidance includes statutory, policy, and procedural requirements and considerations regarding the use of NSLs, administrative subpoenas, grand jury subpoenas, and pen registers. It also includes guidance regarding voluntary disclosures and requests for telephone records of members of the media.

Second, the FBI's response stated that the FBI is in the process of rewriting its policy regarding required legal training for employees and that the policy would require training on the ECPA at least bi-annually. In October 2012, the OIG requested an update from the FBI on this policy. In response to our request, the FBI represented in April 2013 that it is in the process of finalizing an electronic communication that would require all employees who are involved in the process of issuing NSLs to complete the most recent version of the NSL course and the NSL subsystem course in the FBI's Virtual Academy, and thereafter retake these two courses every two years. In addition, the FBI represented that the FBI OGC canvassed the FBI field divisions regarding training provided to FBI employees who work on national security matters and determined that these employees "generally" had received periodic training within the last year on the authorities available to obtain telephone subscriber information and toll billing records. The FBI did not provide information indicating whether such training was required for all personnel involved with issuing such requests.

---

[168] Exigent Letters Report, 45-50, 79-136.

Third, to help ensure the proper acquisition of telephone records in emergency circumstances, the FBI added an electronic form on NSLB's intranet website. The form was designed to standardize and streamline the process by which the FBI generates and tracks requests for voluntary disclosure of ECPA-protected information in emergency situations under 18 U.S.C. § 27O2(b)(8) and (c)(4).

Fourth, the FBI's response stated that in early 2008, the FBI OGC assigned an attorney to work exclusively with the units within the CXS, including the CAU. According to the FBI, the attorney worked closely with CXS personnel, regularly attending the daily CXS Section Chief meetings and other CXS meetings. This attorney interacted with CXS personnel daily and provided guidance regarding all applicable statutes, regulations, and policies such as the ECPA, the FISA, the Attorney General Guidelines, and the DIOG. An Assistant General Counsel in FBI OGC responsible for providing legal support to CAU's successor, TCAU, told the OIG that there are now multiple FBI OGC attorneys that collectively provide this legal support to the TCAU and the other units in the XTS that handle telephonic and electronic communications.

OIG Analysis: We concluded that the DIOG provides necessary and comprehensive guidance on the standards and procedures for obtaining telephone records using available investigative tools. We also believe that the electronic form for voluntary disclosure requests should help ensure that the FBI complies with the requirements of 18 U.S.C. § 2702. However, the OIG requires additional information or action from the FBI before we can determine whether to close this recommendation. The FBI's response to our October 2012 request for an update regarding this recommendation reflects that as of April 2013, the FBI had not implemented its intended policy to require biannual training on NSLs and the NSL subsystem. We believe that the finalization of this policy is necessary to help ensure that all FBI employees who work on national security matters receive periodic training on NSLs. Moreover, since NSLs are only one investigative tool used to acquire ECPA-protected information, we believe the FBI should also expand the training to address the other investigative tools available to the FBI to acquire this information, as set forth in our initial recommendation. Therefore, this recommendation remains resolved but not closed.

Recommendation 3
Status: Closed

OIG Recommendation: We determined that the FBI issued 11 "blanket" NSLs seeking telephone data on over 2,000 telephone numbers in an ill-conceived and ineffective attempt to "cover" or validate the records it

had previously received through exigent letters and other informal means.[169] We also found that CTD officials signed the improper blanket NSLs while serving as Acting Deputy Assistant Directors. At the time these NSLs were signed, the FBI had not issued guidance on whether FBI personnel serving in acting positions were authorized to sign NSLs. To ensure that all FBI personnel serving in acting positions understand what they are authorized or not authorized to approve or sign under various federal statutes, Attorney General Guidelines, and FBI policies, we recommended that the FBI review its guidance to determine if clarification was needed as to the authorities of FBI personnel serving in various acting positions.

FBI Response: On March 27, 2008, the FBI OGC sought guidance from the Office of Legal Counsel on whether officials serving in acting capacities in the Deputy Assistant Director position at Headquarters and the SAC position at a field office may sign NSLs. On January 16, 2009, the OLC issued an opinion concluding that the FBI Director may designate officials serving in those positions on an acting basis to sign NSLs. Thereafter, in September 2009, the FBI issued a policy stating that persons who have been designated in writing to serve in an acting capacity as an SAC, Deputy Assistant Director, or higher-level position may approve NSLs.

In addition, the DIOG contains a general policy regarding the authority of officials serving in an acting capacity. The DIOG permits a supervisor to delegate authority in writing to a supervisor one level below him or her unless prohibited from doing so by statute or other authority. A supervisor may also delegate authority to a higher level supervisor as long as the higher level supervisor is in the original approval chain of command.

OIG Analysis: We believe the FBI's policy governing acting authority for the approval of NSLs and the more general acting authority policy in the DIOG provides appropriate guidance for FBI personnel serving in acting positions. Accordingly, this recommendation is closed.

Recommendations 4 and 5
Status: Closed

OIG Recommendations: In 2003 and 2004, the FBI entered into contracts with the three on-site telephone carriers requiring them to place their employees in the CAU's office space and to give these employees access to their companies' databases so that they could immediately service FBI requests for telephone records. We found that NSLB attorneys did not review these contracts for compliance with the ECPA and other statutes and guidelines until after reviewing a draft of the OIG's first NSL report. As a

[169] Exigent Letters Report, 165-85, 274-76, 285-86.

result, NSLB was unaware of the specific services provided to the CAU, including a feature known as hot number [redacted], which we found was not supported by legal process as required by the ECPA.[170]

Accordingly, we recommended in Recommendation 4 that the FBI OGC review existing contracts between the FBI and private entities or individuals that provide for the FBI's acquisition of telephone records, e-mail records, financial records, or consumer credit records to ensure that the methods and procedures used by the FBI for requesting, obtaining, storing, and retaining these records are in conformity with the NSL statutes and other applicable federal statutes, regulations, Attorney General Guidelines, Executive Orders, and FBI policy. Further, to ensure the legal sufficiency of future contracts, we recommended in Recommendation 5 that the FBI issue a directive requiring that FBI personnel, including FBI OGC attorneys with expertise pertinent to the subject matter of the contract, review contract proposals, responses to requests for contract proposals, and proposed contracts or arrangements with wire or electronic communications service providers.

FBI Response: In its April 1, 2010, response, the FBI represented that a team comprised of NSLB attorneys, privacy attorneys, procurement attorneys, and contracting officers had reviewed the contracts that govern the acquisition of telephone records to ensure they are legally sound. After reviewing the draft of this report, the FBI told the OIG that this review did not include contracts governing the acquisition of e-mail records, financial records, or consumer credit records, as set forth in Recommendation 4, because no such contracts existed.

With respect to Recommendation 5, the FBI established a committee to identify "triggers" that would require contract officers and program managers to submit certain types of procurements – regardless of dollar value – to OGC for review by subject matter legal experts. According to the FBI, the Committee identified contracts for the acquisition of or access to telephone records, electronic communications transaction records, financial records, consumer credit reports, and personally identifiable information (among other things unrelated to these subjects) as warranting review by subject matter experts. On October 14, 2011, the FBI incorporated these triggers into a written policy that requires that certain contracts receive legal review by, and participation throughout the acquisition process from, the FBI OGC.

Further, on January 30, 2013, the FBI provided the OIG with documents reflecting FBI OGC consultation during the contract renewal

[170] Exigent Letters Report, 20-25, 86-87, 286.

process for Company A, Company B, and Company C in 2009 and its approval of the new contracts with Company A and Company C. These documents included e-mail communications between personnel in the Counterterrorism Division and the Chiefs of the FBI OGC's Procurement Law Unit and National Security Law Branch regarding the language in the draft statement of work for each renewal contract. The documents tend to show that procurement and subject matter experts within the FBI OGC reviewed and approved the draft statements of work, which identified the [redacted].

OIG Analysis: The review conducted by a team of NSLB attorneys, privacy attorneys, procurement attorneys, and contracting officers of then-existing contracts governing the acquisition of telephone records to ensure they are legally sound implemented Recommendation 4. In addition, the FBI's policy that sets forth triggers to ensure that subject matter experts within the FBI OGC review certain types of procurements during the acquisition process implemented Recommendation 5. Accordingly, these recommendations are closed.

Recommendation 6
Status: Closed

OIG Recommendation: In our review of the FBI's use of exigent letters, we found that the proximity of the on-site providers' employees to CAU personnel, combined with the lack of guidance, supervision, and oversight of their interactions with FBI employees, contributed to some of the serious abuses identified in our Exigent Letters Report. In response to our findings, in 2008 the FBI removed the on-site providers from CAU space. Nevertheless, given the possibility that the FBI may in the future work with on-site providers, we recommended that if the FBI places employees of communication service providers in the same work space as FBI employees, the FBI issue appropriate guidance and procedures to ensure that the methods and procedures used to obtain records from the providers conform to the ECPA and other applicable authorities.[171]

FBI Response: The FBI has represented that although employees of communication service providers are no longer located in the FBI's office space with FBI employees, if the situation were to change, the FBI would establish appropriate policies, procedures and oversight to ensure compliance with applicable statutes and regulations and to maintain the necessary professional distance between the provider's employees and the FBI's employees.

[171] Exigent Letters Report 25, 287.

OIG Analysis: We believe the FBI has implemented this recommendation by removing on-site communication service provider's employees from CAU work space and agreeing to establish appropriate policies, procedures, and oversight if the FBI places such employees in the same work space as FBI employees in the future. The OIG is therefore closing this recommendation.

Recommendation 7
Status: Open

OIG Recommendation: In our review of the FBI's use of exigent letters, we found that Company A and Company C notified the FBI when [redacted]. This practice was known as hot number [redacted]. The FBI did not provide legal process to Company A or Company C either before or after it [redacted].[172]

During the period covered by our review, the FBI identified 87 "hot numbers" for Company A to monitor and at least 65 hot numbers for Company C to monitor. Company A provided information that [redacted]. We found evidence that Company C may have provided more information than just the existence of calling activity, such as call [redacted].

We concluded that the calling activity information requested by and conveyed to the FBI about these hot numbers required legal process under the ECPA. Although the information given to the FBI by Company A and Company C on these hot numbers was less extensive than the type of information typically provided in response to NSLs or pen register and trap and trace orders, it constituted "a record or other information pertaining to a subscriber or a customer" under the ECPA and, therefore, the providers were prohibited from furnishing the FBI with this information unless a statutory exception to the prohibition applied.[173] We therefore recommended that the FBI issue guidance specifically directing FBI personnel that they may not use practices such as hot number [redacted] to obtain calling activity information from electronic communication service providers.

---

[172] Exigent Letters Report, 79-89, 287.

[173] 18 U.S.C. § 2702(a)(3).

FBI Response: The FBI has represented that this recommendation has been satisfied by the issuance of an FBI policy in June 2009 which, among other things, mandated that "[i]n order to obtain information specific to the subscriber from a provider of electronic communication service to the public, the FBI must provide legal process pursuant to 18 U.S.C. § 2703 or 2709 or the request must fall within those exceptions contained in 18 U.S.C. § 2702 as discussed in this section."[174] The FBI later incorporated this policy into the revised DIOG in October 2011. The FBI told the OIG that hot number [redacted] "would not fall within that policy and is therefore prohibited."

OIG Analysis: We do not believe that the FBI's policy implements our recommendation. To ensure that FBI personnel do not engage in practices known as hot number [redacted], we recommended that the FBI issue guidance that specifically directs FBI personnel that they may not use such practices. Prohibiting the practice by omission falls short of the recommendation, and we believe that it will be a less effective deterrent than a clearly worded prohibition of the practice. Accordingly, this recommendation remains open. Additional information or action from the FBI is required before we can determine whether to close this recommendation.

Recommendation 8
Status: Resolved

OIG Recommendation: In our review of the FBI's use of exigent letters, we found that CAU personnel often asked Company A's on-site employees to conduct so-called community of interest or calling circle searches or analyses on a targeted telephone number whereby they would provide [redacted] the records of the targeted telephone number (first-generation records) [redacted]

---

[174] Section 2703 generally provides that a government entity may require a provider to disclose electronic communications that have been in electronic storage for less than 180 days only by a judicial warrant, but for such communications in electronic storage for longer than 180 days, by an administrative or grand jury subpoena. Section 2703 also provides that a government entity may require a provider to disclose a record or other information pertaining to a subscriber only when the governmental entity obtains a warrant or other legal process, or when the subscriber consents. Section 2709 allows the FBI to compel disclosure of subscriber information and toll billing records information, or electronic communication transactional records, through issuance of an NSL. Section 2702 creates various exceptions to Sections 2703 and 2709. One exception of particular relevance to the Exigent Letters Report allows a provider voluntarily to produce customer records to a government entity "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." 18 U.S.C. § 2702(c)(4).

[redacted]. Company A's employees did not request and the FBI did not provide separate legal process for [redacted]. Instead, they relied upon the initial request for records – an exigent letter, NSL, or grand jury subpoena – containing language requesting a community of interest search.[175]

We also found that in other instances, Company A's employees reviewed [redacted] without a specific request from the FBI. In those instances, if a Company A employee determined that [redacted].

We concluded that the FBI's [redacted] community of interest search practices were improper because the FBI did not establish and certify the relevance of the [redacted] to an authorized national security investigation before requesting or obtaining the information. Further, the decisions about which [redacted] should be searched were made by CAU Intelligence Analysts, supervisory special agents, and special agents, who did not have authority under the ECPA to sign NSLs.

We also concluded that the community of interest search practices used by the FBI were improper because: (1) the FBI did not maintain appropriate documentation to determine under what circumstances and how often these searches were conducted; (2) Company A sometimes provided information pertaining to a subscriber or customer of its service within the meaning of the ECPA without a specific request from the FBI; (3) digital records from Company A did not identify or otherwise distinguish toll billing records for [redacted] were obtained and uploaded into FBI databases without the required certification of an authorized FBI official that the information was relevant to an authorized investigation; and (4) the FBI failed to provide written guidance or establish an approval process for these requests.

Accordingly, we recommended that the FBI issue guidance regarding when FBI personnel may issue [redacted] community of interest search requests. We noted that in November 2007, the CTD prepared draft guidance that would [redacted]

---

[175] Exigent Letters Report, 54-64, 75-78.

[redacted] We recommended that the FBI finalize and issue this policy.

FBI Response: In its April 1, 2010, response, the FBI stated that it "continues to develop policy regarding the circumstances under which [redacted] community of interest search requests may be made." Ultimately, the FBI did not issue the draft policy prepared by CTD in November 2007. Instead, the FBI incorporated specific requirements in the DIOG for [redacted] community of interest search requests made in NSLs.

According to the DIOG, one NSL may [redacted]." The policy requires that the relevance of the [redacted]. Further, the DIOG prohibits [redacted] believe the [redacted]. According to the FBI OGC, since it issued the original DIOG in December 2008, the FBI has made [redacted] community of interest request through NSLs.

The DIOG prohibits the use of an administrative subpoena to simultaneously request [redacted] under any circumstances, but it does not include any requirements or prohibitions concerning the use of grand jury subpoenas to conduct [redacted] community of interest search requests.

OIG Analysis: Although the FBI did not finalize and issue the November 2007 draft policy, we believe it included in the DIOG adequate guidance regarding NSL requests that [redacted]. Like the draft policy, the DIOG requires that the relevance of the [redacted] be established before the records are requested, and that the request be approved by a senior level official. Although the draft policy would have [redacted] we believe that the DIOG's requirement of approval by the Deputy General Counsel for NSLB should ensure meaningful senior level review and approval of these requests. We also believe that the prohibitions in the DIOG against [redacted] if there is reason to believe the [redacted], are appropriate.

It is unclear whether the DIOG provisions concerning relevance, [redacted], and special approval are the only limitations

applicable to [redacted], or whether the DIOG's reference to [redacted] requires consideration by the [redacted] of additional factors before approval can be given. If the latter, we believe the FBI should consider amending the DIOG to identify the other circumstances that must be considered or met before the [redacted] may approve the request.

Further, we believe the FBI should set forth requirements in the DIOG on the use of grand jury subpoenas to [redacted] telephone records. The November 2007 draft policy [redacted], and we have identified no persuasive reason not to incorporate them into the DIOG's requirements. In that regard, although grand jury subpoenas are issued by U.S. Attorney's Offices, we believe the DIOG should provide guidance to agents to assist them in their investigative efforts in coordination with the U.S. Attorney's Offices in grand jury cases. We believe the guidance should address the importance of establishing the relevance of the [redacted] in all cases and the special considerations and requirements that must be met when there is reason to believe the [redacted].

Accordingly, Recommendation 8 is resolved but not closed so that the FBI can provide additional information or take additional action.

Recommendation 9
Status: Closed

OIG Recommendation: Given our findings regarding hot number [redacted], we recommended that the FBI carefully review the circumstances in which FBI personnel had asked the [redacted] hot numbers, and determine whether the FBI had obtained calling activity information under circumstances that trigger discovery or other obligations in any criminal investigations or prosecutions.[176]

FBI Response: According to its April 1, 2010, response, the FBI has examined the circumstances regarding all 39 telephone numbers for which the FBI received information as a result of hot number [redacted]. The FBI determined that its databases contain toll records for 24 of the 39 numbers, and none of the 24 numbers related to any case that has been prosecuted. According to the FBI, because none of the numbers for which the FBI had obtained toll records related to a prosecution, and given the limited information that is conveyed by a hot number [redacted] that is not followed by

[176] Exigent Letters Report, 79-89, 287.

service of an NSL or grand jury subpoena for toll records, the FBI concluded the hot number [redacted] created no discovery or other obligation in any criminal investigation or prosecution. In addition, according to the FBI, there is no exclusionary rule for violations of the ECPA, including its pen register and trap and trace provisions, that could have triggered any discovery obligation in a criminal investigation or prosecution.

OIG Analysis: We believe the FBI implemented this recommendation by identifying the telephone toll records in its possession that were obtained through hot number [redacted] and determining that none of the records related to a criminal prosecution. We are therefore closing this recommendation.

Recommendation 10
Status: Closed

OIG Recommendation: Among the more troubling practices detailed in our Exigent Letters Report, in three media leak investigations the FBI sought, and in two cases received, telephone toll billing records or other calling activity information from on-site providers relating to telephone numbers assigned to media reporters, without meeting the requirements set forth in federal regulation and Department policy for obtaining such records.[177] The records were sought using an exigent letter in one investigation, and through grand jury subpoenas in the second and third investigations. In each instance, we found a failure to seek the information from alternative sources and no attempt to negotiate the voluntary acquisition of the records, provide the appropriate notice, or obtain the approval of the Attorney General as required. Further, the grand jury subpoenas issued in the second and third media leak investigations included language requesting [redacted] community of interest or

[177] Because of the First Amendment interests implicated by compulsory process to obtain reporter's testimony or their telephone records, 28 C.F.R. § 50.10 (2004) requires special approvals and other advance steps before Department employees are permitted to issue subpoenas for reporters' testimony or the production of their telephone records. Specifically, the regulation requires, among other things, that all reasonable attempts be made to obtain the information from alternative sources, that the Department attempt to negotiate the voluntary acquisition of the records with the news media personnel, and that any requests for subpoenas be approved by the Attorney General. The regulation also requires that if the toll records of members of the news media are subpoenaed without the required notice, the affected member of the news media must be notified "as soon thereafter as it is determined that such notification will no longer pose a . . . substantial threat to the integrity of the investigation" and, in any event, within 45 days of any return in response to the subpoena. Department policies supplement this regulation by specifying the information required to be included in requests seeking Attorney General approval for issuance of such subpoenas. *See* United States Attorneys' Manual § 9-13.400, "News Media Subpoenas; Subpoenas for Telephone Toll Records of News Media; Interrogation, Arrest, or Criminal Charging of Members of the News Media."

calling circle records. In addition, in the third investigation, the on-site providers searched their databases for the cell phone records of a reporter without any request from the FBI.[178]

We recommended that the Department determine if, in addition to the grand jury subpoenas identified in our review, the Department has issued other grand jury subpoenas in media leak investigations that included a request for [redacted] community of interest or calling circle searches. We recommended that if such grand jury subpoenas had been issued, the Department should determine whether at the time the subpoenas were issued responsible Department personnel were aware of or suspected contacts between the target numbers in the subpoenas and members of the news media and whether the Department obtained the toll billing records of news reporters in compliance with Department regulations, including the notification requirements.

Response: In its April 13, 2010, response to the Exigent Letters Report, the Department stated that after reviewing relevant materials, neither the NSD nor the Criminal Division had identified any responsive grand jury subpoenas in media leak investigations that were not previously identified by the OIG's review. According to an NSD representative, this review included an examination of all grand jury subpoenas issued in connection with media leak investigations.

OIG Analysis: The Department has implemented this recommendation by conducting a review to determine whether any additional grand jury subpoenas in media leak investigations included a request for [redacted] community of interest or calling circle searches and by representing to the OIG that no such subpoenas had been identified. We are therefore closing this recommendation.

Recommendation 11
Status: Resolved

OIG Recommendation: In connection with the first media leak investigation described in Recommendation 10 above, the FBI conducted [redacted] whose telephone records the FBI had obtained in response to an exigent letter. The FBI agents told [redacted]. Because of the significant First Amendment interests implicated by such [redacted], as well as operational considerations such as obtaining cooperation when necessary in future

[178] Exigent Letters Report, 89-122, 287.

exceptional circumstances, we recommended that the Department re-evaluate the policies governing the conduct of [redacted] and consider under what circumstances FBI personnel may conduct [redacted], including whether approval by senior FBI officials at the level of an Assistant Director or higher should be required for the conduct of such [redacted].[179]

Response: Shortly after the issuance of our Exigent Letters Report, the FBI and the Department stated their intention to review current policies and procedures governing [redacted]. When the FBI reissued the DIOG in October 2011, the FBI incorporated specific procedures for [redacted]. These procedures require: [redacted]. Further, in a circumstance where the [redacted] during the course [redacted], the procedures require that the FBI obtain the approval of the Attorney General pursuant to 28 C.F.R. § 50.10.

OIG Analysis: We believe the procedures in the DIOG for conducting [redacted], including the consultation and approval requirements, are responsive to our recommendation that the Department reevaluate its policies to help ensure that the FBI conducts these [redacted] only after consideration and approval by senior FBI officials. However, on July 12, 2013, the Department issued a report, *Report on Review of News Media Policies*, available at http://www.justice.gov/ag/news-media.pdf, which made revisions to the Department's policies regarding investigations that involve members of the news media. Although this report did not specifically address [redacted], we believe the FBI should consult with the Department to determine whether the recent policy changes warrant any revisions to the DIOG's procedures for conducting [redacted], including the approval level required before such [redacted]. Accordingly, this recommendation is resolved but not yet closed.

---

[179] Exigent Letters Report, 99-102, 251-252, 288.

Recommendation 12
Status: Closed

OIG Recommendation: Based on our concern that the FBI may have used records obtained from exigent letters and other informal methods to seek FISA Court orders, we examined in our exigent letter review a small sample of the FISA Court applications that referred to telephone numbers for which records had been requested from the on-site communications service providers. Our investigation showed that in four cases FBI personnel had filed inaccurate sworn declarations with the FISA Court about the source of subscriber or calling activity information referenced in applications seeking electronic surveillance or pen register and trap and trace orders. Because we reviewed only a small percentage of FISA Court applications that may have relied upon information derived from exigent letters or other improper requests, we recommended that the FBI, in conjunction with the NSD, determine whether any FISA Court orders for electronic surveillance or pen register and trap and trace devices in place at the time of our Exigent Letters Report (in addition to any such orders identified in our report) relied upon FBI statements as to the source of subscriber information for telephone numbers listed in exigent letters or the 11 blanket NSLs. If the FBI and the NSD identified any such orders, we recommended that the FBI and NSD determine whether any of the statements characterizing the source of subscriber information were inaccurate or incomplete. If any such statements were inaccurate or incomplete, we recommended that the FBI and NSD determine whether any of these matters should be referred to the FBI Inspection Division or the Department's Office of Professional Responsibility for further review.

Response: In its April 1, 2010, response, the FBI stated that beginning in 2006, FISA declarations have been subject to a more rigorous fact-checking process than was in place prior to that date. As part of that process, NSD and the FBI conduct "accuracy" reviews of FISA declarations on a regular basis. Agents are required to prepare an "accuracy" file in which the reference material for every factual assertion in a FISA declaration must be retained. According to the FBI, given the passage of time since any exigent letter was used and given the rigorous internal processes designed to ensure accuracy that are now in place, if there had been any misstatements regarding the source of telephone records discussed in any currently operative FISA, that error likely would have already been detected and corrected. The FBI also stated that NSD had committed to determine whether any telephone number appearing on an exigent letter or blanket NSLs was referenced in any current FISA application and "[i]f there are any such declarations, once that universe is determined, depending on available resources, the FBI and NSD will undertake a review of some or all of the declarations to determine whether

any of the statements regarding the source of information regarding such numbers is inaccurate or incomplete."

In its April 13, 2010, response, the NSD stated that it was in the process of identifying the universe of applications that would fall within the scope of our recommendation and that depending on the results of the inquiry and available resources, the NSD and FBI will undertake a review of the applications to determine whether any of the statements characterizing the source of the subscriber information for the identified telephone numbers contain inaccurate or incomplete information.

On February 2, 2013, the Chief of NSD's Oversight Section advised the OIG that the NSD, in conjunction with the FBI, completed a review of the applications falling within the scope of our recommendation. According to the Section Chief, the FBI identified 4,379 telephone numbers as having been listed in an exigent letter or 1 of the 11 blanket NSLs. Using a search protocol, the NSD sought to determine whether any of the 4,379 telephone numbers "have been targeted" in current applications and orders for electronic surveillance or pen register and trap and trace devices and found 1 such number. According to the Section Chief, the NSD determined that the statements in the FISA application as to the source of the subscriber information for that telephone number were accurate.

OIG Analysis: The FBI and the Department implemented this recommendation by completing a review of current FISA applications to determine whether any of the statements characterizing the source of the subscriber information for the 4,379 telephone numbers contained inaccurate or incomplete information. Accordingly, this recommendation is closed.

Recommendation 13
Status: Resolved

OIG Recommendation: After reviewing a draft of our Exigent Letters Report, the FBI for the first time asserted that as a matter of law it [redacted][180] :

[redacted]

[180] Exigent Letters Report, 263-68.

[redacted].

The FBI reads this [redacted] the NSL statute, the [redacted].[181]

The FBI told the OIG that it did not rely on the [redacted] when it sought the records discussed in the Exigent Letters Report. However, before the OIG's report was issued, the FBI OGC asked the OLC for an opinion on the [redacted]. In its request, the FBI OGC stated that [redacted] The OLC also concluded that, [redacted].[182]

The OIG found that the FBI's [redacted] to obtain the type of records it obtained through exigent letters raised important policy concerns. We therefore recommended that the FBI and the Department consider how the FBI [redacted]. We also recommended that the Department

---

[181] In the Exigent Letters Report, we noted two other important distinctions between [redacted]. Exigent Letters Report, 266-67.

[182] The redactions in this paragraph are of information the FBI identified as classified and privileged attorney-client communications.

notify Congress of this issue and of the OLC opinion interpreting the scope of the FBI's authority under it so that Congress can consider the [redacted] and the implications of its potential use.

Response: The FBI stated in its April 1, 2010, response that its policy regarding the issues raised in our recommendation is set forth in the DIOG, which provides that "[redacted] The FBI stated that [redacted] numbers and associated records. The FBI also stated that it had discussed the OLC opinion with staff from the oversight committees in the House and Senate and represented to them that it "is not currently working on policy changes in this regard."

The FBI also said that it represented to the oversight committees and discussed with the Department that if it were to change its policy in response to the OLC opinion, it would do so in consultation with the Department, and that any such change in policy would be limited to requests that target [redacted]. According to the FBI's response, if a [redacted]. The FBI further stated that if a new policy permitted "community of interest" requests for records [redacted], it would [redacted]." Lastly, the FBI stated that it committed to the oversight committees that it would fully brief them in advance of implementing any such changes and that "any such policy would include administrative recordkeeping requirements."

The Associate Deputy Attorney General wrote to the OIG on April 13, 2010, that the FBI's response "reflects the Department's position on this matter." The NSD also stated that "FBI policy does not permit the FBI to use the sort of investigatory methods at issue here and there is no current intent at FBI or elsewhere in the Department to change that policy."

In follow-up interviews and requests for information from NSD officials, the OIG was told that on [redacted], the Attorney General [redacted]. An NSD official told the OIG that these [redacted]

[redacted]

The OIG has requested an update to the information that the NSD provided in 2012 to determine whether the FBI's policy of obtaining remains unchanged. In June 2013, the NSD informally told the OIG that the FBI continues not to seek and, on October 7, 2013, stated in writing to the OIG that this continues to be the case.

OIG Analysis: The OIG recommended that the FBI and the Department consider how the FBI may . The FBI stated in its April 2010 response that its policy concerning the acquisition of transactional records and basic subscriber information was to seek them as provided in 18 U.S.C. §§ 2701-2712, and that the DIOG . Although the FBI stated that , its response suggested to us that the FBI was in the future.

Information provided by the NSD shows that the FBI received authorization to at issue in the Exigent Letters Report and our recommendation, we believe that the FBI's April 2010 response and

[redacted]. Even with regard to telephone billing records, which are the subject of our prior report and recommendation, we believe the better approach would be for the FBI to adopt and disseminate a clear statement in the DIOG that would provide notice to agents and others engaged in obtaining records in this area that FBI personnel should use Sections 2701-2712 of the ECPA to obtain telephone billing records for [redacted]. Therefore, we consider this recommendation resolved and, should the FBI adopt and disseminate a more explicit statement of its policy, we will consider closing the recommendation.

The Department, through the FBI, has satisfied the OIG's related recommendation that it inform Congress of the issue regarding the potential application of the [redacted], and the OLC opinion interpreting the scope of the FBI's authority under it.

II. Conclusions and Recommendations

In this chapter, we examined the FBI and the Department's efforts to implement the recommendations made in our Exigent Letters Report. We determined that the FBI and the Department have fully implemented 8 of 13 recommendations to address the FBI's past use of exigent letters and other informal practices related to telephone records. With respect to the remaining five recommendations, we believe the FBI should take the following steps to fully implement the recommendations in our Exigent Letters Report.

To further address Recommendation 2, the FBI should finalize its intended policy to require all employees who are involved in the process of issuing NSLs to complete training on NSLs and the NSL subsystem every two years and include in this training the other investigative tools available to the FBI to acquire ECPA-protected information.

To address Recommendation 7, the FBI should issue guidance specifically directing FBI personnel that they may not use practices such as hot number [redacted] to obtain calling activity information from electronic communication service providers.

To further address Recommendation 8, the FBI should set forth requirements in the DIOG on the use of grand jury subpoenas to simultaneously request [redacted] telephone records. We believe the requirements should address the importance of establishing the relevance of the [redacted] in all cases and the special considerations and requirements that must be met when there is reason to believe the [redacted].

To further address Recommendation 11, the FBI should consult with the Department to determine whether recent policy changes in the Department's July 12, 2013, *Report on Review of News Media Policies* warrant any revisions to the DIOG's procedures for [redacted].

Finally, to further address Recommendation 13, the FBI should set forth a clear statement in the DIOG that would provide notice to agents and others engaged in obtaining telephone records that FBI personnel should use Sections 2701-2712 of the ECPA to obtain telephone billing records for [redacted].

CHAPTER SEVEN
CONCLUSIONS AND RECOMMENDATIONS

This review is a follow-up to three previous OIG reports concerning the FBI's use of national security letter authorities. In our first and second NSL reports, issued in March 2007 and March 2008, the OIG found repeated instances of the FBI's misuse of NSL authorities during 2003 through 2006. During our first NSL review we also discovered the FBI's practice of issuing exigent letters and using other informal methods to obtain telephone records, instead of using NSLs or other legal process. We addressed these practices in a separate report issued in January 2010.

In this follow-up review, the OIG examined three topic areas. First, we assessed the current status of the FBI and the Department's implementation of the recommendations made in our prior NSL reports, which covered the FBI's use of NSLs during calendar years 2003 through 2006. Second, we examined the FBI's use of NSLs during calendar years 2007, 2008, and 2009. This examination included an assessment of whether corrective measures taken by the FBI and the Department in response to the findings and recommendations of our first and second NSL reports resulted in improved compliance with NSL requirements. Third, we examined the current status of the FBI and the Department's efforts to implement the recommendations made in our prior Exigent Letters Report.

We concluded that the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our past reports and taking additional measures to improve the FBI's compliance with NSL requirements. Our review demonstrated that these efforts have resulted in substantial improvement in NSL compliance.

We believe that the corrective measures that have had the greatest impact on the FBI's compliance with NSL authorities are the development and consolidation of NSL policy and guidance in the Comprehensive NSL Guidance EC and later the DIOG; the mandatory training provided to NSL users and approvers; the implementation of the NSL subsystem; and the periodic inspections of NSL use by the FBI Inspection Division and the national security review teams.

We determined that the FBI and the Department have fully implemented 23 of 28 recommendations from our first and second NSL reports by creating new internal controls, providing guidance and training to FBI personnel, establishing new record-keeping practices, and conducting periodic reviews of NSL usage.

Nevertheless, five recommendations from our first and second NSL reports require additional effort and attention from the FBI to address the accuracy of information entered into the NSL subsystem and the FBI's record-keeping practices. We will consider whether to close these recommendations after the FBI provides additional information or takes the additional steps described in more detail in Chapter Two.

Our review found that during 2007 through 2009 the FBI issued significantly fewer NSL requests than during 2003 through 2006. During 2007 through 2009, the FBI issued 111,144 NSL requests, with an annual average of 37,048. By comparison, the FBI issued approximately 51,051 NSLs per year between 2004 and 2006, and approximately 48,125 NSL requests per year between 2003 and 2006. The factors that may have contributed to the decrease in the FBI's NSL use during 2007 through 2009 are not self-evident from the data we reviewed, though a few people at the FBI told us that because of increased scrutiny on NSL use agents employed alternative investigative tools when possible. The Department's most recent semiannual classified reports to Congress indicate that the FBI's use of NSLs returned to historically typical numbers after 2009.

We found that the vast majority of NSL requests issued during 2007 through 2009 sought telephone and electronic records under the ECPA. We also found that the FBI issued a majority of its NSL requests in furtherance of counterterrorism investigations and a significant number in furtherance of counterintelligence investigations. The FBI issued substantially fewer requests in furtherance of foreign computer intrusion cyber investigations.

Well more than half of the FBI's NSL requests in 2007 through 2009 were generated from investigations of U.S. persons: 12,818, or 64 percent, in 2007; 18,447, or 74 percent, in 2008; and 13,515, or 63 percent, in 2009. This data indicates that the shift reported in our second NSL review toward more NSL requests generated from investigations of U.S. persons as compared to non-U.S. persons – from 39 percent in 2003 to 57 percent in 2006 – continued in 2007 through 2009.

With respect to the effectiveness of NSLs, our interviews of FBI Headquarters officials and field personnel, as well as our examination of case files and the FBI's data on NSL usage, showed that the NSL continued to be an important tool in the FBI's national security investigations conducted in 2007 through 2009. We found that the FBI used NSLs in 2007 through 2009 in the same ways it had used NSLs in previous years. Almost all field personnel we interviewed told us that they used NSLs to identify an investigative subject's associates and to determine whether a subject had suspicious financial activity or was financially susceptible to recruitment or exploitation.

However, FBI personnel reported that beginning in 2009, certain Internet companies refused to provide electronic communication transactional records in response to ECPA NSLs. They reported that this refusal marked a change from past practice and has had a significant impact on the use and effectiveness of ECPA NSLs requesting such records. To address what has become an impasse between the FBI and the Internet companies on the scope of the ECPA NSL statute, the Department has considered proposing legislation that would clarify the FBI's ability to request and obtain electronic communication transaction records under Section 2709(b). In the absence of a legislative amendment, [redacted]

Our compliance review of NSLs issued in 2008 and 2009 revealed that the corrective measures taken by the FBI and the Department in response to the findings and recommendations made in the OIG's first and second NSL reports had a meaningful impact on the FBI's use of NSLs. Although we identified ongoing compliance challenges in certain areas, we found that the corrective measures that have been taken since our prior reviews generally resulted in substantial improvement in the FBI's compliance with NSL requirements.

We believe that the substantial improvement demonstrated in 2008 and 2009 is largely attributable to the FBI's implementation of the NSL subsystem. The NSL subsystem reduces opportunities for human error with drop-down menus, limited choices, and self-populated fields, and ordered tasks and automated notifications ensure that each NSL receives the required legal and supervisory review and approval. Importantly, we identified no potential IOB violations involving subsystem-generated NSLs that cited the wrong statute, requested full credit reports in counterintelligence matters with no counterterrorism nexus, or lacked the approval of an authorized Senior Executive Service official. We found no instances of NSLs failing to describe the records requested or failing to include the required statutory certification. We also found that approval ECs contained the information necessary for Congressional reporting. The reviews conducted by the FBI's Inspection Division and the NSR program demonstrated similar results.

At the same time, the NSL subsystem cannot eliminate FBI errors completely as it relies upon the careful entry of accurate information. For this reason, we believe the FBI's mandatory training on NSL requirements and IOB reporting and the policies and procedures in the Comprehensive NSL Guidance EC and the DIOG deserve considerable credit for the FBI's improved compliance. In addition, periodic inspections of NSL use help ensure that NSL users and approvers remain vigilant in their attention to

NSL authorities and procedures and help to identify new or reoccurring compliance issues that can form the basis for additional guidance and compliance measures.

In short, our review of the FBI's compliance in 2008 and 2009 indicate that the FBI's corrective measures have provided guidance and internal controls on NSL use that did not exist in 2003 through 2006, and these measures resulted in substantial improvement in the FBI's compliance in 2008 and 2009 with NSL requirements.

Nevertheless, the FBI experienced some compliance challenges in 2008 and 2009. We found that the FBI OGC reported 112 NSL-related potential intelligence violations in 34 matters to the IOB for activity that appears to have occurred in 2008 and 2009. Almost a quarter of these violations involved a substantive typographical error in an NSL caused by mistakes in the identification of a telephone number, e-mail address, or social security number for the target of the NSL. These violations demonstrate the importance of careful entry of information into the NSL subsystem. Almost all of the remaining violations involved the FBI's use or uploading of unauthorized information that had been erroneously provided to the FBI.

We found that the greatest compliance challenge for the FBI in 2008 and 2009 was in the identification of unauthorized collections. Even though there are prompts in the NSL subsystem and escalating supervisory reminders to require some level of agent review for overcollection, we found that the FBI had not previously identified and remedied almost 80 percent of the 19 unauthorized collections identified in our sampling. A comparison between this review and our first NSL review revealed that the identification of unauthorized collections was the only category where we found more rather than fewer errors in 2008 and 2009. The reviews conducted by the NSR program demonstrate that this problem was not isolated to the files we reviewed as nearly all of the post-subsystem NSRs documented at least 1 unauthorized collection that had not been remedied by the FBI and a few documented 10 or more. Future training and guidance should provide greater emphasis and specificity in this area.

Another significant compliance issue is the lack of sufficient description in approval ECs of the relevance of the records sought in the NSL to the underlying investigation. While 93 percent of the approval ECs we reviewed did not present this issue, the results of our review, the NSRs, and the FBI's 2009 NSL review demonstrate that the failure to document relevance was the most frequent compliance failure in approval ECs in 2008 and 2009. In December 2009, the FBI made the narrative entry for the relevance description a mandatory field in the NSL subsystem, so that case agents can no longer move to the next step in the NSL process without

completing this step. This enhancement to the NSL subsystem may help focus agents' attention on the need to articulate the relevance of the records to the investigation. Future training and guidance should re-emphasize this element of the approval EC.

In our review, we also found that one or more NSL-related documents were missing from the NSL sub-file in more than half of the case files we reviewed. Future training and guidance should also remind case agents to ensure that all NSL-related documents, including return data, are maintained in the NSL sub-file.

We found significant delays in the FBI OGC's adjudication of potential IOB matters. The FBI OGC took an average of 427 days, or about 14 months, to report the 34 matters to the IOB. In the most egregious example, the FBI OGC took 919 days, or about 2 and a half years, to adjudicate a matter involving what appeared to be a relatively straightforward, compounded overcollection. While the IOB subsystem is an improvement in the FBI OGC's management of the IOB reporting process, we believe it will not address the main causes of the FBI OGC's slow pace in reporting potential intelligence violations to the IOB. The FBI should take additional steps to address the substantial delays in adjudication caused by limited resources and competing priorities.

In addition, we described in Chapter Five other noteworthy issues we encountered during our review related to the FBI's use of NSLs, including the scope of the term "toll billing records" in Section 2709 of the ECPA. We found that the FBI obtains many types of information in response to NSL requests for toll billing records, and it is unclear whether all of them fall within the scope of Section 2709. In particular, we concluded that the ECPA NSL statute does not clearly establish whether two categories of information – [redacted] and consumer identifying information such as dates of birth and social security numbers – fall within the scope of toll billing records. With respect to a third category of information, we concluded that the plain language of the ECPA does not permit the FBI to request or obtain the subscriber information or toll billing records of individuals "associated with" the target of an NSL without a separate certification that those records are relevant to a national security investigation.

In this review, we also observed that the FBI sometimes received records in response to an NSL request after the authorizing investigation had closed or after the authority for the investigation had expired and, in at least one instance, uploaded the information into an FBI database. We believe the FBI should consider implementing a policy that would require the careful balancing of the privacy interests of the individual against the

potential for future investigative value before permitting the uploading into FBI databases of NSL results received after a case has closed or after the authority for the investigation has expired.

Finally, as described in Chapter Six, we examined the FBI and the Department's efforts to implement the recommendations made in our Exigent Letters Report. We found that the FBI and the Department have fully implemented 8 of 13 recommendations we made in our Exigent Letters Report to address the FBI's past use of exigent letters and other informal practices related to ECPA-protected telephone records. Five recommendations require additional effort and attention from the FBI or the Department. As to three of those recommendations, we found that the FBI should take additional steps to enhance its training and guidance on certain aspects of the ECPA.

In addition, we determined that the FBI should take further steps to address our recommendation concerning [redacted]. In our Exigent Letters Report, we found that the FBI conducted [redacted] the FBI had obtained in response to an exigent letter. The FBI agents [redacted]. Because of the significant First Amendment interests implicated by such [redacted], as well as operational considerations such as obtaining cooperation when necessary in future exceptional circumstances, we recommended that the Department re-evaluate the policies governing the [redacted] and consider under what circumstances FBI personnel may conduct [redacted], including whether approval by senior FBI officials at the level of an Assistant Director or higher should be required for the conduct of [redacted].

Since that time, on July 12, 2013, the Department issued a report, *Report on Review of News Media Policies*, which made revisions to the Department's policies regarding investigations that [redacted]. Although this report did not specifically address [redacted], we believe the FBI should consult with the Department to determine whether the recent policy changes warrant any revisions to the DIOG's procedures for conducting [redacted], including the approval level required before such [redacted].

The remaining recommendation in our Exigent Letters Report that is resolved but not closed concerns the FBI's potential [redacted] to obtain telephone billing records [redacted]. The

[redacted] provides, in pertinent part, that notwithstanding the Stored Communications Act and certain other statutes, the U.S. Government may acquire:

[redacted]

The FBI reads [redacted] the NSL statute, [redacted] that requests for such information be approved by senior officials or that its use be reported to Congress.

The OIG's concern about this potential use was based on the fact that records [redacted] may also contain [redacted]. Since issuance of the Exigent Letters Report, the OIG has requested information from the FBI and the Department about the FBI's use of the [redacted]. In June 2013, the Department informally told the OIG that the FBI [redacted]. On October 7, 2013, the Department confirmed in writing to the OIG that the FBI still does not use the [redacted].

Meanwhile, the FBI has stated that its current policy in the DIOG is that the FBI may acquire telephone subscriber and transactional records as provided in Sections 2701-2712 of the ECPA, the provisions that require a government entity to obtain such records from a provider through legal process, or voluntarily if a provider in good faith believes that emergency circumstances warrant the disclosure. The FBI told the OIG that this policy [redacted]. The FBI also stated that if it were to change this policy, it would do so in consultation with the Department. However, we believe that FBI policy should more clearly state that FBI personnel should use Sections 2701-2712 of the ECPA to obtain telephone billing records for [redacted].

We will consider whether to close these recommendations after the FBI provides additional information or takes the additional steps described in more detail in Chapter Six.

In sum, our review found that the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our past reports and taking additional measures to improve the FBI's compliance with NSL requirements. We found that the FBI fully implemented 31 of 41 recommendations from our first and second NSL reports and our Exigent Letters Report. Our review demonstrated that these efforts have resulted in substantial improvement in the FBI's compliance with NSL authorities. We found that 10 recommendations from our prior reports require additional information or attention, and we identify steps the FBI and the Department should take to address them. In addition, because we identified compliance challenges in certain areas, we made 10 new recommendations to the FBI and the Department to further improve the use and oversight of NSLs. We recommend that:

1. The FBI should provide periodic training and guidance re-emphasizing the importance of (1) sending NSL-related documents, including NSL return data, to the appropriate NSL sub-file, and (2) properly documenting and scrutinizing the predication for the investigation, the relevance of the specific records requested in the NSL to the investigation, and the justification for the invocation of the non-disclosure provisions in the approval EC.

2. The FBI should take steps to ensure that case agents and supervisors assigned to national security investigations are aware of and adhere to FBI OGC guidance pertaining to the identification of information that is beyond the scope of an NSL request, including providing additional training and assuring that the guidance contained in the FBI OGC's *NSL Collection Chart* is well publicized and easily accessible.

3. Notify the President's Intelligence Oversight Board concerning the unauthorized collections found in this review containing [redacted] from two providers and seek guidance on whether the FBI should undertake the effort necessary to identify and remove similar unauthorized collections that likely remain in many FBI case files.

4. The FBI should upgrade the NSL subsystem in the FISA Management System to require that case agents verify whether NSL return data matched the information requested in the NSL and whether it contained an overcollection. In addition, the FBI should consider an upgrade that would require that case agents make the same entries in the NSL subsystem for the return data of manually generated NSLs as are required for subsystem generated NSLs and send escalating e-mail notifications when those entries are not made.

5. The FBI should reconsider whether Section 1681f of the FCRA prohibits a consumer reporting agency from voluntarily providing the FBI with an NSL target's date of birth, social security number, or telephone number in response to a FCRA NSL under Section 1681u, and provide additional guidance as appropriate.

6. The FBI should take additional steps to address the substantial delays in the FBI OGC's adjudication of potential IOB matters caused by limited resources and competing priorities.

7. In future NSL compliance reviews, the FBI Inspection Division should incorporate the examination of two additional data points: (1) the extent to which NSL documents are maintained in the appropriate NSL sub-file; and (2) with respect to uncompounded third party errors, whether the FBI took the appropriate remedial measures in conformity with FBI policies and procedures.

8. The FBI and the Department should revive their efforts to bring about a legislative amendment to Section 2709 by submitting another proposal that defines the phrase "toll billing records." We believe the legislative proposal should specify the categories of telephone and electronic records the Department seeks to have Congress define as falling within the scope of ECPA Section 2709, in order to ensure that the FBI does not seek or obtain information to which it is not authorized. We believe that in devising any new legislative proposal, the Department should consider whether the [redacted], and consumer identifying information such as dates of birth and social security numbers, should be included among those the Department seeks to have specifically included within the scope of Section 2709. Finally, because a legislative change may take time, we believe the Department should simultaneously seek a legal opinion from the OLC on whether the information described in Chapter Five and in the FBI's template attachment to ECPA NSLs falls within the scope of Section 2709.

9. The FBI should take steps to ensure that it does not request or obtain "associated" records without a separate determination and certification of relevance to an authorized national security investigation. These steps should include, but not necessarily be limited to, the incorporation of guidance in the Domestic Investigations Operations Guide and in training materials making clear that before seeking "associated" records in an NSL, the relevant FBI officials must make a separate determination and certification that those records are relevant to an authorized national security investigation.

10. The FBI should consider implementing a policy that would require agents, in consultation with FBI OGC attorneys, to carefully balance

the privacy interests of the individual against the potential for future investigative value before permitting the uploading into FBI databases of NSL return data received after a case has closed or after the authority for the investigation has expired.

APPENDICES

NOTE: Appendices A through D are not attached to the public version of the report because the FBI determined the information contained in the appendices is classified.

APPENDIX E

PAGE INTENTIONALLY LEFT BLANK

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

June 25, 2014

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U. S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, *A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Progress in Implementing Recommendations and Examination of Use in 2007 through 2009.*

We are pleased that you found that "the FBI and the Department have devoted considerable resources toward implementing the recommendations made in our past reports and [are] taking additional measures to improve the FBI's compliance with NSL requirements." We are also pleased that the OIG has concluded that 31 of the 41 recommendations from the prior NSL reports have been fully implemented. With respect to the remaining recommendations, the OIG has noted our substantial progress and has requested further action. In the attached responses we detail actions we have taken or plan to take to achieve full implementation.

With respect to the OIG's compliance review of NSLs from calendar years 2007-2009, the OIG has noted that the corrective measures taken by the FBI and the Department have resulted in "substantial improvement in the FBI's compliance with NSL authorities." During the past five years the FBI has continued or increased its efforts to enhance compliance with NSL requirements. For example, during calendar years 2010, 2011, 2012, and 2013, attorneys from the FBI and the Department's National Security Division conducted 65 National Security Reviews in FBI field offices nationwide. The reviewers examined national security investigations to ensure compliance with the Constitution, applicable statutes, Attorney General Guidelines, and FBI policy directives. Among other things, during these reviews they examined NSLs for relevancy, overproduction, and appropriate approvals. In addition, more than 10,000 FBI employees completed the FBI's comprehensive online training course for NSLs in 2008 (the year the online course was first implemented). Between 2009 and 2012, an average of 1,400 employees took the course each year. Given these recent activities, we believe that NSL compliance in current FBI cases is likely even higher.

The FBI and Department's commitment to ensure NSLs are issued in full adherence to the law remains steadfast. The FBI and Department will work to bring closure to the remaining recommendations and continue to internally audit NSLs on an annual basis to identify any additional areas for corrective action.

In conclusion, the FBI wishes to thank your review team for their work and for their continuing efforts to provide helpful input to the FBI.

Sincerely,

Richard McNally
Acting Deputy General Counsel for the
National Security Law Branch
Federal Bureau of Investigation

FBI Response to the OIG NSL III Report Recommendations

FIVE RECOMMENDATIONS FROM THE NSL I AND II REPORTS

Recommendation 6, NSL I (Resolved); and Recommendation 17, NSL II (Resolved)

Discussion of Recommendations 6 (NSL I) and Recommendation 17 (NSL II) in the NSL III Report (NSL III Report, pp. 39-44)

> (U) We will consider closing these recommendations upon receipt of further information and documents from the FBI establishing that the FBI has considered, and will consider in the future, the feasibility of electronic tagging as it adopts new systems that process NSL-derived information. (NSL III Report, p. 44.)

FBI Response to NSL III Report

> (U) Concur. The DOJ/ODNI NSL Retention Working Group ("Working Group"), chaired by the DOJ Chief Privacy and Civil Liberties Officers, examined issues regarding NSL retention and considered the OIG Recommendation 6 from NSL I and Recommendation 17 from NSL II. Working with the FBI and NSD, the Working Group drafted recommendations that dealt with the concerns raised by the OIG. In October 1, 2010, Attorney General Eric Holder adopted the Working Group's recommendations and promulgated the *Procedures for Collection, Use and Storage of information Derived from National Security Letters*. The Attorney General's policy specifically addressed the OIG concerns about the FBI's use of its NSL authorities and financial data received pursuant to the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5); credit data received pursuant to the Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681u and 1681v; and subscriber information, toll billing records, and electronic communication transactional records received pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709. The policy was designed to ensure that only those records that may have "investigative value"[1] are included in the FBI central recordkeeping system.
>
> (U) Concerning tagging, the NSL Working Group concluded that it would be prohibitively expensive to retrofit existing FBI systems to provide for electronic tagging. Nonetheless, the FBI adopted a tagging structure for NSL-derived information for its Telephone Applications, which marks information uploaded into the FBI Telephone Applications as being derived from an NSL. In addition, when viewing or exporting the records from Telephone Applications the records are marked with an NSL flag, thereby noting the records are derived from an NSL.

---

[1] (U) "Investigative value" means the information responds to or creates a new investigative need, contributes to an intelligence collection requirement or has the reasonable potential to provide other FBI or Intelligence Community (IC) employees information of value consistent with their mission. *Procedures for Collection, Use and Storage of information Derived from National Security Letters* (March 1, 2010), p.1, FN 1.

(U) Therefore, the FBI has complied with the OIG's Recommendation 6, NSL I Report (March 2007, p. 126) to "[c]onsider measures" concerning FBI agents and analysts in handling NSL-derived information and using the information in analytical intelligence products, and the FBI has also complied with the OIG's Recommendation 17, NSL II Report (March 2008, p. 163) to "re-examine measures for [] addressing the privacy interests associated with NSL-derived information, including the benefits and feasibility of labeling or tagging NSL-derived information, and [] minimizing the retention and dissemination of such information." The FBI will also continue to consider in the future the feasibility of electronic tagging of NSL-derived information as it adopts new systems that process such information. Accordingly, the OIG should close Recommendation 6 from the NSL I Report (March 2007) and Recommendation 17 from the NSL II Report (March 2008).

Recommendation 12, NSL II (Resolved)

Discussion of Recommendation 12 (NSL II) in the NSL III Report (NSL III Report, pp. 44–47, and 52)

(U) The revised DIOG provides that supervisors should consider during file reviews whether NSLs, if any, have been issued in accordance with NSL policy, including whether NSL return data has been reviewed for overcollection. The revised DIOG does not state that supervisors should ensure that NSL-related documents are in the appropriate NSL sub-file. Accordingly, we believe the FBI should consider providing additional guidance to the field to ensure compliance with this requirement and revising the template for the case file review reports to have each case agent state whether all NSL-related documents are in the NSL sub-file. We therefore consider Recommendation 12 resolved but not yet closed. (NSL III Report, p. 47.)

...

(U) Finally to further address Recommendation 12 in our second NSL report, the FBI should consider issuing additional guidance to the field to ensure that squad supervisors understand their responsibility to verify adherence to NSL record-keeping requirements during quarterly case file reviews and revise the template for the case file review reports to have each case agent state whether all NSL-related documents are in the NSL sub-file. (NSL III Report, p. 52.)

FBI Response to NSL III Report

(U) Concur. The FBI will consider issuing additional guidance to squad supervisors concerning quarterly case file reviews. The FBI will also consider revising the template for the case file review reports to include whether the documents are in the NSL sub-file.

(U) Concur. The FBI will consider issuing additional guidance to squad supervisors to verify adherence to NSL record-keeping requirements during quarterly case file reviews.

(U) The FBI will also consider revising the template for the case file review reports to include whether the NSL-related documents are in the hard NSL sub-file, to the extent that a hard sub-file exists, recognizing that increasingly NSL sub-files and their accompanying records are stored digitally in an FBI central recordkeeping system. The Domestic Investigations and Operations Guide (DIOG) Section 18.6.6.3.11 RETENTION OF NSL INFORMATION provides that "[redaction]."

(U) For the signed NSL itself, FBI DIOG Section 18.6.6.3.7.2 COPY OF THE NSL AND RELATED DOCUMENTS IN THE INVESTIGATIVE FILE, now reads: "[redaction]" (Emphasis in original.) For NSLs created outside FISAMS, DIOG Section 18.6.6.3.7.2 reads, "[redaction]." (Emphasis in original.) If the signed NSL is not serialized, then "[redaction]" Section 18.6.6.3.7.2 COPY OF THE NSL AND RELATED DOCUMENTS IN THE INVESTIGATIVE FILE).

Recommendation 2, NSL II (Resolved)

Discussion of Recommendation 2 (NSL II) in the NSL III Report (NSL III Report, pp. 47-48, and 52)

(U) [W]e note throughout this report, the NSL subsystem cannot eliminate FBI errors completely and instead must rely upon the careful entry of accurate information. It is still necessary, for example, that a case agent enter the correct U.S. person status of the investigative subject and NSL target when generating an NSL in the subsystem. We continue to believe the FBI should consider incorporating in the FBI Inspection Division's NSL reviews an examination of a sample of the data entries made in the NSL subsystem, including the entries made in connection with manually generated NSLs, to evaluate and help ensure the accuracy of the information entered into the subsystem. Accordingly, this recommendation is resolved but remains open so that the FBI may provide additional information or take additional steps to address this recommendation. (NSL III Report, p. 48.)

...

(U) To further address Recommendation 2 in our second NSL report, the FBI should consider incorporating in the FBI Inspection Division's NSL reviews an examination of a sample of the data entries made in the NSL subsystem, including the entries made in connection with manually generated NSLs, to evaluate and help ensure the accuracy of the information entered into the subsystem. (NSL III Report, p. 52.)

FBI Response to NSL III Report

(U) Concur. The FBI Inspection Division will consider incorporating into its NSL reviews an examination of a sample of the data entries made in the NSL subsystem,

including entries made in connection with manually generated NSLs, to evaluate the accuracy of the information entered into the subsystem.

Recommendation 3, NSL II (Resolved)

Discussion of Recommendation 3 (NSL II) in the NSL III Report (NSL III Report, pp. 19-21, and 51)

> (U) [W]e believe the certification requirement in the NSL subsystem should require the case agent to attest not only that the information contained in the request is factually accurate, but also that the information identifying the target (for example, telephone number, e-mail or IP address, social security number, or bank account number) has been verified with source documents in the case file. (NSL III Report, p. 21.)
>
> ...
>
> (U) Therefore, to further reduce substantive typographical errors, we believe the FBI should consider the efficacy of an upgrade that would require the user to enter the target's identifying information into the subsystem twice and not accept the information when the entries do not match. (NSL III Report, p. 21.)

FBI Response to NSL III Report

> (U) Concur. The FBI will consider the efficacy of upgrading the FISA Management System (FISAMS) to require the user to enter the target's identifying information into the subsystem twice and not accept the information when the entries do not match. Concerning the case agent attesting that the request is factually accurate, FISAMS already requires the case agent to certify the information contained in the request is factually accurate. Finally, the FBI will consider the efficacy of upgrading FISAMS to require the case agent when attesting that the information contained in the request is factually accurate to also affirm that the target's identifying information has been verified with the source.

FIVE RECOMMENDATIONS FROM THE EXIGENT LETTERS REPORT

Recommendation 2, Exigent Letters Report (Resolved)

Discussion of Recommendation 2 (Exigent Letters Report) in the NSL III Report (NSL III Report, pp. 166-167)

> (U) The FBI's response to our October 2012 request for an update regarding this recommendation reflects that as of April 2013, the FBI had not implemented its intended policy to require biannual training on NSLs and the NSL subsystem. We believe that the finalization of this policy is necessary to help ensure that all FBI employees who work on national security matters receive periodic training on NSLs. Moreover, since NSLs are only one investigative tool used to acquire ECPA-protected information, we believe the FBI should also expand the training to address the other investigative tools available to the FBI to acquire this information, as set forth in our initial recommendation. Therefore, this recommendation remains resolved but not closed. (NSL III Report, p. 167.)

FBI Response to NSL III Report

> (U) Concur. The FBI adopted a policy on September 26, 2013, requiring all FBI employees who work on national security matters to complete periodic training on NSLs and the NSL subsystem through the FBI Virtual Academy. Therefore, that portion of Recommendation 2 from the Exigent Letters Report (January 19, 2010) should be closed.
>
> (U) Concerning periodic training for investigative tools used to acquire ECPA-protected information besides NSLs, the FBI will consider expanding its training on the Pen Register Act, the federal regulation governing subpoenas for toll billing records of reporters, and the FBI's administrative subpoena authorities.

Recommendation 7, Exigent Letters Report (Open)

Discussion of Recommendation 7 (Exigent Letters Report) in the NSL III Report (NSL III Report, pp. 171-173)

> (U) We do not believe that the FBI's policy implements our recommendation. To ensure that FBI personnel do not engage in practices known as hot number [redaction], we recommended that the FBI issue guidance that specifically directs FBI personnel that they may not use such practices. Prohibiting the practice by omission falls short of the recommendation, and we believe that it will be a less effective deterrent than a clearly worded prohibition of the practice. Accordingly, this recommendation remains open. Additional information or action from the FBI is required before we can determine whether to close this recommendation. (NSL III Report, pp. 172-173.)

FBI Response to NSL III Report

(U) Concur. As the OIG notes, the FBI does not use the practice of hot number [redaction]. The FBI will consider issuing guidance that reaffirms to FBI personnel not to use hot number [redaction] so that the OIG may close Recommendation 7.

Recommendation 8, Exigent Letters Report (Resolved)

Discussion of Recommendation 8 (Exigent Letters Report) in the NSL III Report (NSL III Report, pp. 173-175)

(U) It is unclear whether the DIOG provisions concerning relevance, [redaction], and special approval are the only limitations ... or whether the DIOG's reference to "[redaction]" requires consideration by the [redaction] of additional factors before approval can be given. If the latter, we believe the FBI should consider amending the DIOG to identify the other circumstances that must be considered or met before the [redaction] may approve the request. (NSL III Report, p. 175.)

FBI Response to NSL III Report

(U) Concur. The FBI DIOG was recently amended to incorporate the OIG's recommendations. The DIOG now reads:

18.6.6.3.7 (U) SPECIFIC PROCEDURES FOR CREATING NSLs

A) (U) [redaction].

(U) The DIOG revision eliminated the phrase "[redaction]" and codified FBI practice that the [redaction] must approve such requests in addition to the other approval layers that already exist for NSLs. Therefore, the FBI having now complied with Recommendation 8 from the Exigent Letters Report (January 19, 2010), the recommendation should be closed.

Recommendation 11, Exigent Letters Report (Resolved)

Discussion of Recommendation 11 (Exigent Letters Report) in the NSL III Report (NSL III Report, pp. 178-179)

(U) We believe the procedures in the DIOG for conducting [redaction], including the consultation and approval requirements, are responsive to our recommendation that the Department reevaluate its policies to help ensure that the FBI conducts these [redaction] only after consideration and approval by senior FBI officials. However, on July 12, 2013, the Department issued the *Report on Review of News Media Policies*, available at

http://www.justice.gov/ag/news-media.pdf, which made revisions to the Department's policies regarding investigations that involve members of the news media. Although this report did not specifically address [redaction], we believe the FBI should consult with the Department to determine whether the recent policy changes warrant any revisions to the DIOG's procedures for conducting [redaction], including the approval level required before such [redaction]. Accordingly, this recommendation is resolved but not yet closed. (NSL III Report, p. 179.)

FBI Response to NSL III Report

(U) Concur. The FBI will consult with the Department officials to determine whether the recent policy changes warrant revision to the FBI DIOG.

Recommendation 13, Exigent Letters Report (Resolved)

Discussion of Recommendation 13 (Exigent Letters Report) in the NSL III Report (NSL III Report, pp. 181-184.)

(U) [W]e believe ... the FBI [should] adopt and disseminate a clear statement in the DIOG that would provide notice to agents and others engaged in obtaining records in this area that FBI personnel should use Sections 2701-2712 of the ECPA to obtain telephone billing records for either [redaction]. Therefore, we consider this recommendation resolved and, should the FBI adopt and disseminate a more explicit statement of its policy, we will consider closing the recommendation. (NSL III Report, p. 184.)

FBI Response to NSL III Report

(U) Concur. As the OIG has recognized, the FBI relies on Title 18, United States Code, Sections 2701-2712 of the Electronic Communications Privacy Act to obtain toll billing records. The FBI will consider adding a statement in the FBI DIOG that obtaining telephone billing records should be pursuant to Title 18, United States Code, Sections 2701-2712 of the Electronic Communications Privacy Act, so that the OIG may close the recommendation.

TEN RECOMMENDATIONS FROM THE NSL III REPORT

Source: NSL III Report, pp. 193-195.

Recommendation 1. (U) The FBI should provide periodic training and guidance re-emphasizing the importance of (1) sending NSL-related documents, including NSL return data, to the appropriate NSL sub-file, and (2) properly documenting and scrutinizing the predication for the investigation, the relevance of the specific records requested in the NSL to the investigation, and the justification for the invocation of the nondisclosure provisions in the approval EC. (NSL III Report, p. 193.)

FBI Response

(U) Concur. The FBI has already taken action to implement same, to wit:

- Through an Electronic Communication (EC) adopted by the FBI on September 9, 2013, the FBI affirmatively took steps requiring all employees who work on national security matters to complete periodic training on NSLs and the NSL subsystem through the FBI Virtual Academy.

- New sections have been added to the FBI DIOG that emphasize even more than before the requirement to send NSL-related documents, including NSL return data, to the NSL sub-file (Section 18.6.6.3.9 RECEIPT OF NSL INFORMATION, REVIEW FOR OVERPRODUCTION, AND RELEASING THE INFORMATION, and Section 18.6.6.3.11 RETENTION OF NSL INFORMATION).

- The FBI now provides periodic training and guidance re-emphasizing the importance of (1) sending NSL-related documents, including NSL return data, to the appropriate NSL sub-file; and (2) properly documenting and scrutinizing the predication for the investigation, the relevance of the specific records requested in the NSL to the investigation, and the justification for the invocation of the nondisclosure provisions in the approval EC.

- The new FBI DIOG now includes more information about properly documenting and scrutinizing the predication for the investigation prior to issuing an NSL (Section 18.6.6.3.3 APPROVAL REQUIREMENTS, and Section 18.6.6.3.4 STANDARDS FOR ISSUING NSLs).

- The new FBI DIOG now includes more information concerning the relevance of the specific records requested in the NSL to the investigation (Section 18.6.6.3.3 APPROVAL REQUIREMENTS, Section 18.6.6.3.4 STANDARDS FOR ISSUING NSLs, and Section 18.6.6.3.7 SPECIFIC PROCEDURES FOR CREATING NSLs).

- The new FBI DIOG now includes more information about the justification for the invocation of the nondisclosure provisions in the approval EC (Section 18.6.6.3.3

APPROVAL REQUIREMENTS, Section 18.6.6.3.7 SPECIFIC PROCEDURES FOR CREATING NSLs, and Section 18.6.6.3.7.1 COVER EC APPROVING AN NSL.)

(U) Therefore, the FBI has now complied with Recommendation 1 and the recommendation should be closed.

Recommendation 2. (U) The FBI should take steps to ensure that case agents and supervisors assigned to national security investigations are aware of and adhere to FBI OGC guidance pertaining to the identification of information that is beyond the scope of an NSL request, including providing additional training and assuring that the guidance contained in the FBI OGC's NSL Collection Chart is well publicized and easily accessible. (NSL III Report, p. 193.)

FBI Response

(U) Concur. To ensure that case agents and supervisors assigned to national security investigations are aware of and adhere to FBI OGC guidance pertaining to the identification of information that is beyond the scope of an NSL request, the FBI has now posted on its NSL webpage the Collection Chart and discusses it in NSL training. FBI OGC included a presentation about the chart at the FBI Annual CDC Conference in 2012 and 2013, and will do so at future CDC Conferences. A hard copy of the chart was provided to the CDCs at the FBI Annual CDC Conference in 2012 and 2013, and will also be distributed at future CDC Conferences. All NSLB attorneys have a copy of the chart to use for advising FBI employees on NSL matters. Access to the chart is available through the NSL webpage to employees across the FBI who work on national security matters. The FBI has now provided the additional training and information as well as provided specific bureau-wide training pertaining to the identification of information that is beyond the scope of an NSL request, and, therefore, Recommendation 2 should be closed.

Recommendation 3. (U) Notify the President's Intelligence Oversight Board concerning the unauthorized collections found in this review containing [redaction] information from two providers and seek guidance on whether the FBI should undertake the effort necessary to identify and remove similar unauthorized collections that likely remain in many FBI case files. (NSL III Report, pp. 193-194.)

FBI Response

(U) Concur. The FBI will notify the President's Intelligence Oversight Board (IOB) about the information that third parties mistakenly provided to the FBI when complying with an NSL request as third party overproduction that was neither used nor serialized by the FBI. The FBI will also discuss with the Board whether the FBI should undertake the effort necessary to identify and remove the overproduction.

Recommendation 4. (U) The FBI should upgrade the NSL subsystem in the FISA Management System to require that case agents verify whether NSL return data matched the information requested in the NSL and whether it contained an overcollection. In addition, the FBI should consider an upgrade that would require that case agents make the same entries in the NSL subsystem for the return data of manually generated NSLs as are required for subsystem generated NSLs and send escalating e-mail notifications when those entries are not made. (NSL III Report, pp. 194.)

FBI Response

(U) Concur. To help ensure case agents verify whether NSL return data matches the information requested in the NSL and therefore does not contain overproduction, the FISA Management System (FISAMS) now requires agents when completing the Specify Return in the Ordered Tasks to confirm the NSL results do not contain overproduction. That requirement now also exists for NSLs manually generated outside FISAMS. Therefore, the FBI has now complied with that portion of Recommendation 4 and that portion of the recommendation should be closed.

(U) Concerning asking agents whether the "NSL return data match[es] the information requested," agents now verify in FISAMS that overproduction does not exist when they complete the Specify Return in the Ordered Task confirming the NSL results do not contain overproduction. Therefore, the FBI has now complied with that portion of Recommendation 4 and that portion of the recommendation should be closed.

(U) For the remaining portion of Recommendation 4 concerning upgrading FISAMS to extend the escalating e-mail notifications to include NSLs manually generated, the FBI will consider the efficacy of doing so.

Recommendation 5. (U) The FBI should reconsider whether Section 1681f of the FCRA prohibits a consumer reporting agency from voluntarily providing the FBI with an NSL target's date of birth, social security number, or telephone number in response to a FCRA NSL under Section 1681u, and provide additional guidance as appropriate. (NSL III Report, p. 194.)

FBI Response

(U) Concur. The FBI will reconsider whether a consumer reporting agency may voluntarily provide the FBI with the date of birth, social security number, or telephone number of the target of an NSL when responding to an NSL issued under the Fair Credit Reporting Act when the NSL does not list date of birth, social security number, or telephone number, and the FBI will also provide additional guidance to the field as appropriate.

Recommendation 6. (U) The FBI should take additional steps to address the substantial delays in the FBI OGC's adjudication of potential IOB matters caused by limited resources and competing priorities. (NSL III Report, p. 194.)

FBI Response

(U) Concur. The FBI has now taken additional steps to address the substantial delays in the FBI OGC's adjudication of potential IOB matters. To ensure the timely adjudication of potential IOB matters continues, the FBI has now developed and implemented a new automated FISAMS IOB subsystem to improve the reporting of potential IOB violations and information about overproduction. The new IOB subsystem's automated workflow helps ensure the consistency and completeness of reports to the FBI OGC by prompting FBI personnel through each step of the reporting process. In addition, the new time requirements for the preparation and review of adjudication memoranda, along with the new e-mail notification that alerts NLSB attorneys when the requirements are not met, have reduced the time taken to adjudicate potential IOB matters. Pursuant to a request from the IOB, the FBI now reports on potential IOB matters that occur within a given quarter no later than 60 days after the end of the quarter. The FBI backlog of IOB matters has been reduced to less than 100. Pursuant to guidance from the IOB, the FBI has prioritized resources on adjudication of current potential IOB matters, though it also continues to address the backlog, too. The FBI has now taken the steps that provide for the timely adjudication of potential IOB matters and, therefore, Recommendation 6 should be closed.

Recommendation 7. (U) In future NSL compliance reviews, the FBI Inspection Division should incorporate the examination of two additional data points: (1) the extent to which NSL documents are maintained in the appropriate NSL sub-file; and (2) with respect to uncompounded third party errors, whether the FBI took the appropriate remedial measures in conformity with FBI policies and procedures. (NSL III Report, p. 194.)

FBI Response

(U) Concur. The FBI Inspection Division incorporated into its 2013 NSL compliance review an examination of the extent to which NSL documents are maintained in the appropriate NSL sub-file and, and with respect to uncompounded third party errors, whether the FBI took the appropriate remedial measures in conformity with FBI policies and procedures. The FBI Inspection Division will continue to include them in future reviews. The FBI has now complied with Recommendation 7 and, therefore, the recommendation should be closed.

Recommendation 8. (U) The FBI and the Department should revive their efforts to bring about a legislative amendment to Section 2709 by submitting another proposal that defines the phrase "toll billing records." We believe the legislative proposal should specify the categories of telephone and electronic records the Department seeks to have Congress define as falling within the scope of ECPA Section 2709, in order to ensure that the FBI does not seek or obtain information to which it is not authorized. We believe that in devising any new legislative proposal, the Department should consider whether the specific [redaction], and consumer identifying information such as dates of birth and social security numbers, should be included among those the Department seeks to have specifically included within the scope of Section

2709. Finally, because a legislative change may take time, we believe the Department should simultaneously seek a legal opinion from the OLC on whether the information described in Chapter Five and in the FBI's template attachment to ECPA NSLs falls within the scope of Section 2709. (NSL III Report, p. 194.)

FBI Response

(U) Concur. The FBI agrees that clarity to Section 2709 will be helpful and the FBI will continue to support efforts for legislative action in this regard. Concerning submitting legislative proposals, the FBI and the Department do not submit legislative proposals to Congress. For the executive branch, the President decides whether to submit legislative proposals to Congress, usually after – as has been done with the proposal concerning 18 U.S.C. § 2709 – a department-wide review process has been completed. In the case of Section 2709, that department-wide review process has been completed and the President will decide whether, and if so when, to submit a legislative proposal to Congress. The FBI agrees with the OIG's concern that accomplishing a legislative change may take time. To resolve the matter until a legislative change is accomplished, the FBI and the Department have agreed that as a matter of policy the FBI will now treat dates of birth and social security numbers provided by third parties responding to NSLs seeking toll billing records as third party overproduction if the FBI does not include dates of birth or social security numbers in the NSL. Finally, concerning the attachment to ECPA NSLs, the FBI has now removed it from the models used to create NSLs outside FISAMS, and the FBI is in the process of removing it from NSLs created in FISAMS. The FBI and the Department have now complied with Recommendation 8 and, therefore, the recommendation should be closed.

Recommendation 9. (U) The FBI should take steps to ensure that it does not request or obtain "associated" records without a separate determination and certification of relevance to an authorized national security investigation. These steps should include, but not necessarily be limited to, the incorporation of guidance in the Domestic Investigations Operations Guide and in training materials making clear that before seeking "associated" records in an NSL, the relevant FBI officials must make a separate determination and certification that those records are relevant to an authorized national security investigation. (NSL III Report, p. 195.)

FBI Response

(U) Concur. The FBI has now removed the phrase "associated records" from the models used to create NSLs outside FISAMS, and the FBI is in the process of removing it from NSLs created in FISAMS.

(U) Concerning changing the FBI DIOG to incorporate guidance that records obtained with an NSL must be relevant to an authorized national security investigation, the new DIOG now more than ever discusses across multiple sections that records obtained with an NSL must be relevant to an authorized national security investigation, to wit:

1. Section 18.6.6.1 OVERVIEW OF COMPULSORY PROCESS

2. Section 18.6.6.2 APPLICATION
3. Section 18.6.6.3.2 DEFINITION OF METHOD
4. Section 18.6.6.3.3 APPROVAL REQUIREMENTS
5. Section 18.6.6.3.4 STANDARDS FOR ISSUING NSLs
6. Section 18.6.6.3.7 SPECIFIC PROCEDURES FOR CREATING NSLs
7. Section 18.6.6.3.7.1 COVER EC APPROVING AN NSL
8. Section 18.6.6.3.9 RECEIPT OF NSL INFORMATION, REVIEW FOR OVERPRODUCTION, AND RELEASING THE INFORMATION
9. Section 18.6.6.3.10 OVERPRODUCTION
10. Section 18.6.6.3.14 SPECIAL PROCEDURES FOR HANDLING RIGHT TO FINANCIAL PRIVACY ACT INFORMATION AND OTHER INFORMATION.

(U) Concerning changing FBI training materials to remove references to "associated" records, the FBI NSL training materials for NSLs do not reference "associated" records.

(U) Therefore, the FBI has now complied with Recommendation 9 and the recommendation should be closed, except for the portion concerning FBI removing the phrase "associated records" from NSLs created in FISAMS. That portion of Recommendation 9 should remain open. After the FBI has completed that portion of the recommendation, the FBI will inform the OIG so that Recommendation 9 may be closed.

Recommendation 10. (U) The FBI should consider implementing a policy that would require agents, in consultation with FBI OGC attorneys, to balance carefully the privacy interests of the individual against the potential for future investigative value before permitting the uploading into FBI databases of NSL return data received after a case has closed or after the authority for the investigation has expired. (NSL III Report, p. 195.)

FBI Response

(U) Concur. The FBI will consider implementing a policy that would require balancing the privacy interests of the individual against the potential for future investigative value before serializing into the FBI's central recordkeeping system NSL return data received after a case has closed or after the authority for the investigation has expired.