A Review of the FBI's Use of National Security Letters:
Assessment of Corrective Actions and Examination of NSL Usage in 2006

Office of the Inspector General
March 2008

UNCLASSIFIED

TABLE OF CONTENTS

TABLE OF CONTENTS i

INDEX OF CHARTS AND TABLES v

LIST OF ACRONYMS vii

CHAPTER ONE: INTRODUCTION 1

I. Provisions of the Patriot Act and Patriot Reauthorization Act 2

II. Methodology of the OIG Review 3

III. Organization of the Report 5

IV. Summary of OIG Findings 6

CHAPTER TWO: STATUS OF THE FBI'S AND DOJ'S CORRECTIVE ACTIONS IN RESPONSE TO THE OIG'S FIRST NSL REPORT 13

I. Overview of the FBI's and Department's Corrective Measures 14

II. Status of the FBI's Implementation of the OIG's Recommendations in Our First NSL Report 19

III. Other Corrective Measures Implemented by the FBI and Other Department Components 49

A. The FBI's Office of Integrity and Compliance 49

1. Organization Structure and Operations 50
2. Risk Assessment Process 52
3. OIG Analysis 53

B. National Security Division 55

1. Office of Intelligence 55
2. Oversight Section 57
3. OIG Analysis 63

C. National Security Letter Working Group 64

1. Evaluation of Existing Controls and Guidelines 65
2. Additional Privacy Enhancements Recommended by the NSL Working Group 66
3. Other Enhancements Considered but Not Recommended 68

4. OIG Analysis of the NSL Working Group's Report and Recommendations 69

IV. OIG Conclusions and Recommendations 72

CHAPTER THREE: THE FBI'S 2007 REVIEWS OF NATIONAL SECURITY LETTERS IN RESPONSE TO THE OIG'S FIRST NSL REPORT 75

I. The FBI's 2007 Reviews of National Security Letters 77

A. The FBI's 2007 Field Review of National Security Letters 77

1. Methodology of the FBI's 2007 Field Review 78
2. The FBI's Post-Field Work Analysis 79
3. The FBI's Findings 81
4. Comparison of Findings in the FBI's 2007 NSL Field Review and the OIG's First NSL Report 85

B. The FBI's 2007 Headquarters Review of NSLs 86

1. Background 86
2. FBI Methodology 87
3. The FBI's Headquarters Findings 87

C. The FBI's Review of FCRA NSLs Seeking Consumer Full Credit Reports in Counterintelligence Investigations 89

1. The OIG's Findings on FCRA NSLs in Our First NSL Report 89
2. The FBI's 2007 Review of FCRA NSLs 90

II. The OIG's Analysis of the FBI's 2007 NSL Reviews 93

A. The OIG's Verification of the FBI's 2007 Field Review of NSLs 93

1. The OIG's Methodology 94
2. Findings of the OIG's Review 94

B. OIG Analysis 98

1. The OIG's Conclusions Regarding the Field and Headquarters Reviews 98
2. The OIG's Conclusions Concerning the FBI's FCRA Review 101

III. OIG Conclusions and Recommendations 102

CHAPTER FOUR: NATIONAL SECURITY LETTER REQUESTS ISSUED BY THE FBI IN 2006 104

I. Methodology 105

II. National Security Letter Requests Issued in 2006 107

III. Trends in National Security Letter Usage from 2003 through 2006 109

CHAPTER FIVE: THE EFFECTIVENESS OF NATIONAL SECURITY LETTERS AS AN INVESTIGATIVE TOOL 114

CHAPTER SIX: OIG FINDINGS ON THE FBI'S COMPLIANCE WITH THE PATRIOT REAUTHORIZATION ACT'S NON-DISCLOSURE AND CONFIDENTIALITY PROVISIONS 117

I. Background 117

A. The Patriot Reauthorization Act 117

B. The FBI's Implementation of the Patriot Reauthorization Act Non-Disclosure and Confidentiality Requirements 119

C. Methodology of the OIG Review 121

1. Random Sample of NSLs Issued After March 9, 2006 121
2. Other 2006 NSLs Identified During the Review 123

II. OIG Findings and Analysis 124

A. NSLs That Invoked Non-Disclosure and Confidentiality Obligations 124

B. NSLs That Did Not Invoke Non-Disclosure and Confidentiality Obligations 126

C. "Blanket" NSLs Issued in 2006 127

III. OIG Conclusions and Recommendation 128

CHAPTER SEVEN: IMPROPER OR ILLEGAL USE OF NATIONAL SECURITY LETTERS REPORTED BY FBI PERSONNEL IN 2006 131

I. The FBI Process for Reporting Possible Violations Involving Intelligence Activities in the United States 134

A. The Process for Reporting Possible Intelligence Violations 134

B. FBI Guidance on Reporting and Adjudicating Possible Intelligence Violations 135

1. November 16, 2006, Guidance on Reporting Possible IOB Violations to the FBI OGC 135

2. November 30, 2006, Guidance to FBI OGC NSLB Attorneys Adjudicating Possible IOB Violations 136

II. Possible Intelligence Violations Arising From National Security Letters Reported to the FBI OGC in 2006 137

A. Possible NSL-Related IOB Violations Reported to the IOB in 2006 139

B. OIG Analysis Regarding Possible NSL-Related IOB Violations Reported to the IOB 145

C. Possible NSL-Related IOB Violations Not Reported to the IOB in 2006 146

D. OIG Analysis of Possible NSL-Related IOB Violations Not Reported to the IOB 148

E. Comparison of Possible NSL-Related IOB Violations Reported to the FBI OGC in 2006 and from 2003 through 2005 152

III. OIG Conclusions and Recommendations 155

CHAPTER EIGHT: CONCLUSIONS AND RECOMMENDATIONS 157

UNCLASSIFIED APPENDIX A-1

CLASSIFIED APPENDIX B-1

INDEX OF CHARTS AND TABLES

		Page
Chart 2.1	Organization of the Office of Intelligence	56
Chart 3.1	Comparison of Possible NSL-Related IOB Violations Identified in the OIG's First NSL Report and the FBI's 2007 Field Review	86
Chart 3.2	Comparison of Possible NSL-Related IOB Violations Identified by the FBI and the OIG (by category) in NSLs Reviewed in Three Field Offices	96
Chart 4.1	Relationship between Investigations, NSLs, and NSL Requests in 2006	105
Chart 4.2	NSL Requests (2006)	108
Chart 4.3	NSL Requests Relating to Investigations of U.S. Persons and non-U.S. Persons (2006)	108
Chart 4.4	NSL Requests in Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations (2006)	109
Chart 4.5	NSL Requests (2003 through 2006)	110
Chart 4.6	NSL Requests Relating to U.S. Persons and non-U.S. Persons (2003 through 2006)	112
Chart 4.7	NSL Requests in Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations (2003 through 2006)	113
Chart 6.1	NSLs that Imposed Non-Disclosure and Confidentiality Obligations (March 10, 2006 through December 31, 2006)	124
Chart 7.1	Possible NSL-Related IOB Violations Reported to the FBI OGC (2003 through 2006)	138
Chart 7.2	Timeliness of 34 FBI Field Reports to the FBI OGC of Possible NSL-Related IOB Violations Reported to the IOB (2006)	144
Table 3.1	NSL-Related Infractions Identified in the FBI's 2007 Field Review Later Classified by the FBI as "Administrative Errors"	81
Table 3.2	Possible NSL-Related IOB Violations Identified in the FBI's 2007 Field Review (2003 through 2006)	83
Table 3.3	Possible NSL-Related IOB Violations Identified in the FBI's 2007 Headquarters Review (2003 through 2006)	88

		Page
Table 3.4	Possible FCRA IOB Violations Identified in the FBI's 2007 Review of NSLs Issued in Counterintelligence Investigations (2002 through 2006)	92
Table 3.5	Possible NSL-Related IOB Violations Identified by the OIG Not Identified by FBI Inspectors at Three Field Offices During the FBI's 2007 Field Review	95
Table 3.6	Comparison of Possible NSL-Related IOB Violations Identified by the FBI and the OIG at Three Field Offices	96
Table 7.1	Summary of 84 Possible NSL-Related IOB Violations Reported to the FBI OGC (2006)	139
Table 7.2	Summary of 34 NSL-Related IOB Violations Reported to the IOB by the FBI OGC (2006)	140
Table 7.3	Summary of 50 Possible NSL-Related IOB Violations Not Reported to the IOB (2006)	146
Table 7.4	Comparison of Possible NSL-Related IOB Violations Reported to the FBI OGC (2003 through 2005 and 2006)	153

LIST OF ACRONYMS

ACS	Automated Case Support System
ADC	Assistant Division Counsel
CAU	Communications Analysis Unit
CDC	Chief Division Counsel
CTD	Counterterrorism Division
DNI	Director of National Intelligence
EAD	Executive Assistant Director
EC	Electronic Communication
ECPA	Electronic Communications Privacy Act
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FISA	Foreign Intelligence Surveillance Act of 1978
IIS	Internal Investigations Section
IOB	Intelligence Oversight Board
ISP	Internet Service Provider
JTTF	Joint Terrorism Task Force
NARA	National Archives and Records Administration
NSB	National Security Branch
NSD	National Security Division
NSI	National Security Investigations
NSL	National Security Letter
NSLB	National Security Law Branch
OGC	Office of the General Counsel
OIC	Office of Integrity and Compliance
OIG	Office of the Inspector General
OIPR	Office of Intelligence Policy and Review
OLC	Office of Legal Counsel
OPR	Office of Professional Responsibility
RFPA	Right to Financial Privacy Act
SAC	Special Agent in Charge
TFOS	Terrorist Financing Operations Section

CHAPTER ONE:
INTRODUCTION

The *USA PATRIOT Improvement and Reauthorization Act of 2005* (Patriot Reauthorization Act or the Act) directed the Department of Justice (Department or DOJ) Office of the Inspector General (OIG) to review, among other things, "the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice."[1] The Act required the OIG to conduct reviews on the Federal Bureau of Investigation's (FBI) use of national security letters (NSL) for two separate time periods.[2]

The OIG's first report on the FBI's use of NSLs, issued on March 9, 2007, covered calendar years 2003 through 2005.[3] This is the OIG's second report on the FBI's use of NSLs. In this report we describe and assess the response by the FBI and the Department to the serious misuse of NSL authorities that our first report described. In addition, as required by the Patriot Reauthorization Act, this report describes the FBI's use of NSLs in calendar year 2006.

We are also in the process of completing an investigation of the FBI's use of exigent letters, a practice that we described generally in our first NSL report. This investigation also will assess responsibility for the improper use of these exigent letters. We are nearing the end of that investigation on the use of exigent letters, and we intend to issue a report covering this subject in the near future.

---

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

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

[2] The Patriot Reauthorization Act also directed the OIG to conduct reviews on the use and effectiveness of Section 215 orders for business records, another investigative authority that was expanded by the Patriot Act. The results of the OIG's first review on Section 215 orders are contained in a report issued on March 9, 2007. The OIG's second review of Section 215 orders in 2006 is contained in a separate report issued in conjunction with this report.

[3] U.S. Department of Justice Office of the Inspector General, *Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 9, 2007) (NSL I), available at www.doj.gov/oig. We refer to the unclassified version of that report as the first NSL report. Although the Act required the OIG to include only calendar years 2003 through 2004 in the first report, we elected to also include 2005 in that report.

I. Provisions of the Patriot Act and Patriot Reauthorization Act

In the Introduction of our first NSL report, we described the expansion of the FBI's national security letter authorities in the USA PATRIOT Act (Patriot Act) and do not repeat that description here.[4] However, for this report on the FBI's use of NSL authorities in 2006, we first identify the issues that the Patriot Reauthorization Act directed the OIG to review:

> (1) an examination of the use of national security letters by the Department of Justice during calendar year 2006;
>
> (2) a description of any noteworthy facts or circumstances relating to such use, including any improper or illegal use of such authority; and
>
> (3) an examination of the effectiveness of national security letters as an investigative tool, including –
>
> > (A) the importance of the information acquired by the Department of Justice to the intelligence activities of the Department of Justice or to any other department or agency of the Federal Government;
> >
> > (B) the manner in which such information is collected, retained, analyzed, and disseminated by the Department of Justice, including any direct access to such information (such as access to "raw data") provided to any other department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;
> >
> > (C) whether, and how often, the Department of Justice utilized such information to produce an analytical intelligence product for distribution within the Department of Justice, to the intelligence community . . ., or to other Federal, State, local, or tribal government departments, agencies or instrumentalities;
> >
> > (D) whether, and how often, the Department of Justice provided such information to law enforcement authorities for use in criminal proceedings; . . . .[5]

---

[4] NSL I, 10-16. The term "USA PATRIOT Act" is an acronym for the law entitled the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56 (2001). This law is commonly referred to as "the Patriot Act."

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

With respect to national security letters issued following the date of enactment of the Patriot Reauthorization Act (March 9, 2006), the Act also directed the OIG to examine:

> (E) the number of occasions in which the Department of Justice, or an officer or employee of the Department of Justice, issued a national security letter without the certification necessary to require the recipient of such letter to comply with the nondisclosure and confidentiality requirements potentially applicable under law.

II. Methodology of the OIG Review

To describe and assess the status of the FBI's implementation of its response to the recommendations made in our first NSL report, additional corrective actions taken by the FBI and other Department components, and the FBI's use of national security letters in 2006, the OIG conducted interviews of over 30 current and former FBI and Department employees, including personnel at FBI Headquarters in the Office of the General Counsel (FBI OGC), Counterterrorism Division, Counterintelligence Division, and Cyber Division; and personnel in 3 field offices: Baltimore, Miami, and Washington, D.C. We examined over 18,000 FBI documents and pieces of digital information provided by FBI Headquarters operational and support divisions and the 3 field divisions. Among the documents we analyzed were FBI Headquarters guidance memoranda; correspondence; national security letters; reports by the FBI's Inspection Division, the FBI OGC, and the Department's Office of Professional Responsibility; information posted on the FBI's Intranet; e-mails; and training materials on the use of NSLs.

To examine the progress of the FBI's implementation of the 11 recommendations in our first NSL report, we analyzed the FBI's memoranda describing the status of its corrective actions. We also interviewed FBI officials from the FBI OGC and Inspection Division, other senior FBI officials including the FBI Director and Deputy Director, and field personnel responsible for issuing and reviewing NSLs including the Special Agents in Charge (SAC), Chief Division Counsels (CDC), Supervisory Special Agents, and Special Agents. Additionally, we reviewed all NSL-related guidance issued by the FBI since our first report was issued, reviewed the types of NSL training provided and to whom it was provided, and observed a demonstration of the new NSL data system that was designed to manage and track NSLs.

We also examined other corrective actions and new oversight measures implemented in 2007 by the FBI, the Department's National Security Division (NSD), and the Office of the Deputy Attorney General relating to the use of NSLs. These measures included the FBI's establishment of an Office of Integrity and Compliance (OIC) and the NSD's new compliance reviews, called "national security reviews," which review the FBI's use of NSL authorities and other intelligence techniques in national security investigations. We interviewed NSD and FBI personnel responsible for these reviews and examined relevant documents describing the establishment of the OIC and the national security reviews. In addition, we evaluated the August 2007 report and proposal to the Attorney General by the Department's Chief Privacy and Civil Liberties Officer which recommended how the FBI should use and retain NSL-derived information.

The OIG also visited three field offices to assess the accuracy of the FBI's review of NSLs issued by these field offices, initiated after the issuance of our March 2007 report. The FBI's review assessed a random sample of 10 percent of all national security investigations active at any time from 2003 through 2006. We re-examined case files that had been reviewed by FBI inspectors during the FBI's March 2007 field review to verify the accuracy of the data collected by the FBI's review and compared our findings to the FBI's findings.

In addition, in response to the statutory directive to identify the number of occasions in which the Department issued national security letters without the applicable certification necessary to require the recipients to comply with the non-disclosure and confidentiality requirements of the Patriot Reauthorization Act, we reviewed a random sample of all NSLs issued from March 10, 2006, through December 31, 2006, to determine whether these NSLs complied with this requirement. For purposes of assessing compliance with the new legislation, we also analyzed 11 so-called "blanket" national security letters issued after March 9, 2006, that were not part of the random sample but which we identified in the course of another part of our review and which will be described in our forthcoming NSL report.

Finally, to document the FBI's usage of NSLs in calendar year 2006, as required by the Patriot Reauthorization Act, we analyzed data in the FBI OGC database. We also examined the Department's annual public reports to evaluate NSL requests in 2006 and to analyze trends in NSL usage from 2003 through 2006.

III. Organization of the Report

This report is divided into eight chapters. This first chapter contains the background to this report, the organization and methodology of the report, and a summary of the report's findings.

Chapter Two evaluates the FBI's specific responses to the 11 recommendations we made in our first NSL report. In this chapter, we also examine the FBI's new OIC, the NSD's new procedures for auditing compliance with NSL authorities and other techniques used in national security investigations, and the report by the Department's Chief Privacy and Civil Liberties Officer regarding the use and retention of information obtained through NSLs.

Chapter Three describes steps taken by the FBI in response to our March 2007 report, including three reviews the FBI initiated following release of our first NSL report:

> (1) its review of NSLs issued by FBI field offices from a random sample of 10 percent of all national security investigations active at any time from 2003 through 2006;
>
> (2) a separate review of 10 percent of NSLs issued by FBI Headquarters divisions during the same period; and
>
> (3) a review of NSLs issued in FBI counterintelligence investigations pursuant to the *Fair Credit Reporting Act* (FCRA) from 2002 through 2006.

Chapter Four presents the data on the FBI's use of national security letters in 2006. This information is based on data derived from the FBI OGC national security letter tracking database and the Department's semiannual classified reports to Congress on NSL usage.

Chapter Five addresses the effectiveness of national security letters in 2006.

Chapter Six presents our findings on the number of occasions in which the Department issued national security letters without the certifications necessary to require the recipients of such letters to comply with the non-disclosure and confidentiality requirements of the Patriot Reauthorization Act.

Chapter Seven describes several instances of improper or illegal use of national security letter authorities in 2006. These include the matters self-reported by FBI Headquarters and field personnel to the FBI OGC in 2006.

Chapter Eight contains our conclusions and recommendations.

The Unclassified Appendix to the report contains comments on the report by the Attorney General, the Director of National Intelligence, the Assistant Attorney General for the National Security Division, and the FBI. The classified report also contains a Classified Appendix.

As noted above, the OIG will soon issue another NSL report that will describe the results of our investigation of the FBI's use of exigent letters to obtain telephone records from three communication service providers from 2002 through 2006. The report, which will expand on the general findings in our first NSL report on the use of exigent letters in 2003 through 2005, will examine the practice of using exigent letters rather than NSLs or other legal process to obtain records from the three communication service providers, the types of investigations for which records were sought, the process used to obtain the records, and inaccurate statements in many of the letters. The report also will describe the types of records obtained from the three communication service providers and how FBI agents and analysts handled and used the information obtained in response to these letters. The report will describe the FBI's efforts to issue legal process after the fact to cover information previously obtained from the exigent letters; the issuance of 11 "blanket" NSLs in 2006, and other improper NSLs; and the use of less formal types of requests to obtain records from the three communication service providers, such as verbal requests, e-mails, and telephone calls – only some of which were later documented in exigent letters or legal process. In addition, the report will evaluate the responsibility of FBI personnel who signed exigent letters and blanket NSLs and the responsibility of their supervisors and FBI officials. Finally, we will evaluate the processes that led to the issuance of exigent letters, improper blanket NSLs, and other improper NSLs and improper requests for information.

IV. Summary of OIG Findings

Our review concluded that, since issuance of our March 2007 report, the FBI and the Department have made significant progress in implementing the recommendations from that report and in adopting other corrective actions to address serious problems we identified in the use of national security letters. The FBI has also devoted significant energy, time, and 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.

Our interviews of senior FBI officials, including the Director, the Deputy Director, and the General Counsel, indicate that the FBI's senior

leadership is committed to correcting the serious deficiencies in the FBI's use of NSLs identified in our first report. They have attempted to reinforce throughout all levels of the FBI the necessity of adhering to the rules governing the use of NSL authorities.

For example, among other measures the FBI has issued needed guidance on the use of NSLs, provided mandatory training to FBI employees on the proper use of NSLs, and developed a new data system to facilitate the issuance of NSLs and improve the accuracy of NSL data in required congressional reports. The FBI has issued numerous NSL policies and guidance memoranda on topics that include the proper usage of NSLs and statutory and procedural authorizations and restrictions; a prohibition on use of exigent letters; the requirement for sufficient and independent supervisory and legal reviews; and the procedures for identifying and reporting possible intelligence violations.

The FBI has also created a new Office of Integrity and Compliance (OIC), modeled after private sector compliance programs, to ensure that national security investigations and other FBI activities are conducted in a manner consistent with appropriate laws, regulations, and policies. We believe this office can perform a valuable function by providing a process for identifying compliance requirements and risks, assessing existing control mechanisms, and developing and implementing better controls to ensure proper use of NSLs. However, we recommend that the FBI consider providing the OIC with a larger permanent staffing level so that it can develop the skills, knowledge, and independence to lead or directly carry out the critical elements of this new compliance program.

In addition to the FBI's efforts to address the OIG's recommendations, the Department's National Security Division (NSD) has implemented additional measures to promote better compliance with NSL authorities and to address other issues raised by our first report. For example, in 2007 the NSD began reviews to examine whether the FBI is using various intelligence techniques, including NSLs, in accordance with applicable laws, guidelines, and policies.

Also, 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 convened a working group to examine how NSL-derived information is used and retained by the FBI, with special emphasis on the protection of privacy interests, and in August 2007 sent a report and proposal to the Attorney General on minimization procedures with respect to NSL-derived data. However, after review of this proposal, we concluded that the NSL Working Group's report did not adequately address measures to label or tag NSL-derived information and to minimize the retention and dissemination of such information. In February 2008, the Acting Chief

Privacy and Civil Liberties Officer told us that the proposal had been withdrawn and that he intends to reconvene the NSL Working Group to reconsider the August 2007 report and proposal. We examine the August 2007 report of the NSL Working Group and make recommendations for the NSL Working Group to consider as it revises that proposal.

In this report, we also examine the three reviews conducted by the FBI in 2007 following release of our first report. The FBI's reviews confirmed that the types of deficiencies identified in our first NSL report had occurred throughout the FBI from 2003 through 2006. The FBI's field review was important because it covered a larger, statistically valid sample of NSLs and case files. The FBI reviews confirmed similar types of possible intelligence violations in the FBI's use of NSLs that we found. However, the FBI's field review found a higher overall possible IOB violation rate (9.43 percent) than the OIG found (7.5 percent) in the sample we examined in our first NSL report.

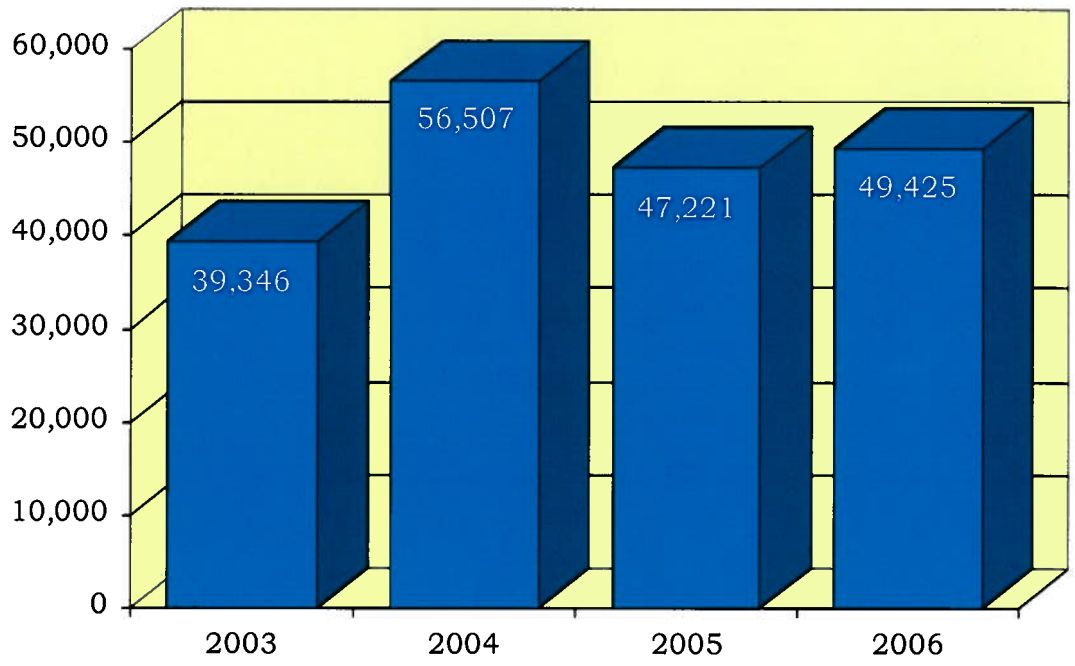
However, we examined in detail the FBI's field review and determined that it did not capture all NSL-related possible intelligence violations in the files it reviewed, and therefore did not provide a fully accurate baseline from which to measure future improvement in compliance with NSL authorities. For example, during our re-examination of case files that FBI inspectors determined had no NSL-related possible intelligence violations in three field offices, we identified 15 additional NSL-related possible intelligence violations. In addition, because FBI inspectors were unable to locate information provided in response to a significant number of NSLs chosen for review in its sample, the results of the FBI's field review likely understated the rate of possible intelligence violations.

In short, despite the significant challenges facing the FBI in eliminating fully shortcomings in its use of NSLs, we believe the FBI and the Department have evidenced a commitment to correcting the problems we found in our first NSL report and have made significant progress in addressing the need to improve compliance in the FBI's use of NSLs. However, because only 1 year has passed since the OIG's first NSL report was released and some measures are not fully implemented or tested, we believe it is too early to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with NSLs that we identified. We believe the FBI must implement all of our recommendations in the first NSL report, demonstrate sustained commitment to the steps it has taken and committed to take to improve compliance, implement additional recommendations described in this second report, consider additional measures to enhance privacy protections for NSL-derived information, and remain vigilant in holding FBI personnel accountable for properly preparing and approving NSLs and for handling responsive records appropriately.

Finally, as required by the Patriot Reauthorization Act, this report details the FBI's use of national security letters in calendar year 2006. It is important to note that the FBI's use of NSLs in 2006 occurred before we issued our first NSL report in March 2007, which identified the serious deficiencies in the FBI's use of and oversight of NSLs, and before the FBI began to implement corrective actions. Therefore, not surprisingly, this report contains similar findings to our March 2007 report regarding deficiencies in the FBI's use of NSLs.

As shown in Chart 4.5, we determined that the FBI's use of national security letters in 2006 continued the upward trend we identified in our first NSL report that covered the period 2003 through 2005. In 2006, the FBI issued 49,425 NSL requests, a 4.7-percent increase over NSL requests issued in 2005. For the 4-year period 2003 through 2006, the FBI issued a total of 192,499 NSL requests.

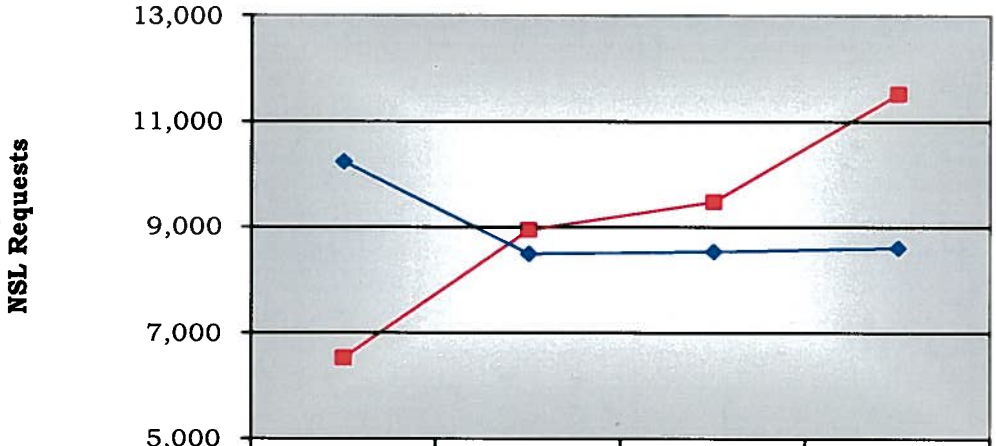
CHART 4.5
NSL Requests (2003 through 2006)



Sources: DOJ semiannual classified reports to Congress and FBI OGC database as of May 2006 (for 1681v NSL requests in 2003 through 2005)

As shown in Chart 4.6, the percentage of NSL requests generated from investigations of U.S. persons continued to increase significantly, from approximately 39 percent of all NSL requests issued in 2003 to approximately 57 percent of all NSL requests issued in 2006.

CHART 4.6
NSL Requests Relating to U.S. Persons and non-U.S. Persons (2003 through 2006)



	2003	2004	2005	2006
Non-U.S. Persons	10,232	8,494	8,536	8,605
U.S. Persons	6,519	8,943	9,475	11,517

Source: DOJ semiannual classified reports to Congress

In our interviews, FBI field and Headquarters personnel told us that NSLs continued to be an indispensable investigative tool in major terrorism and espionage investigations conducted in 2006. They reported that NSLs were used to identify the financial dealings of investigative subjects, confirm the identity of subjects, support the use of sophisticated intelligence techniques, and establish predication for the initiation of preliminary and full counterterrorism and counterintelligence investigations.

As directed by the Patriot Reauthorization Act, we also conducted an audit of the number of occasions in which NSLs issued after the effective date of the Act did not contain the certifications necessary to require the recipients to comply with applicable non-disclosure and confidentiality requirements. The vast majority of the NSLs and approval memoranda we examined, which are known as electronic communications (EC), substantially complied with the Patriot Reauthorization Act certification requirement and FBI policy. We believe this compliance record was largely due to the prompt guidance the FBI OGC issued on the date the Act was signed, the availability of new NSL forms on its Intranet website, and periodic guidance FBI OGC attorneys provided to the field as questions arose. We found that only 10 NSLs (3 percent of a random sample of 375 NSLs we examined) were issued without the required certifications. Our audit also determined that 97 percent of the NSLs in the random sample imposed non-disclosure and confidentiality obligations on recipients.

However, we also determined that 17 NSL approval memoranda (5 percent of the random sample) contained insufficient explanations to justify imposition of these obligations. We identified eight NSLs in our sample that contained recitals about non-disclosure that were inconsistent with the corresponding approval memoranda, signifying that case agents, their supervisors, and Chief Division Counsels were not careful in reviewing and approving these documents to ensure consistency. In addition to these non-compliant NSLs that were part of the random sample, we identified eight "blanket" NSLs issued by senior Counterterrorism Division officials in 2006 that did not contain the required certifications.

To assess any "improper or illegal use" of NSLs in 2006, as required by the Patriot Reauthorization Act, we examined the reports of possible intelligence violations involving the use of NSLs that were sent to the FBI OGC from January 1, 2006, through December 31, 2006. We identified 84 possible intelligence violations involving the use of NSLs, of which the FBI determined that 34 needed to be reported to the President's Intelligence Oversight Board (IOB).[6] The 34 matters included the same types of errors identified in our first NSL report that was completed in March 2007, such as the issuance of NSLs without proper authorization, improper requests, and unauthorized collection of telephone or Internet e-mail records. Of these 34 intelligence violations, 20 were the result of FBI errors, while 14 resulted initially from mistakes by recipients of the national security letters. We generally agreed with the FBI's decisions on which violations needed to be reported to the IOB, except for six that we believed should have been reported to the IOB but were not. We concluded that the decisions not to report these were inconsistent with prior FBI OGC decisions or that the reasons for not reporting them to the IOB were unpersuasive.

As we did in our first NSL report, we determined whether the FBI would have been entitled to the information provided under applicable NSL statutes, Attorney General Guidelines, and internal policies. We found that of the 84 possible intelligence violations identified and reported to the FBI OGC in 2006, the FBI received information it was not entitled to receive in 14 matters. In one of the matters the FBI requested information it was not entitled to under the applicable NSL statute. In the other 13 matters, the FBI made proper requests but, due to third party errors, obtained information it was not entitled to receive under the pertinent NSL statutes.

---

[6] Of the 84 possible intelligence violations, 52 involved the FBI's acquisition of information it had not requested in the NSLs (referred to as "initial third party errors"). Since the FBI OGC has not yet determined whether the FBI compounded the third party errors by using or uploading the unauthorized information, we could not reach a conclusion as to whether these 52 matters involved improper use of NSL-derived information.

This report makes 17 recommendations regarding the FBI's continued use of NSLs. For example, two recommendations are designed to remind FBI case agents and supervisors to carefully examine the circumstances surrounding the issuance of each NSL to determine whether there is adequate justification for imposing non-disclosure and confidentiality requirements on the NSL recipient and to ensure that NSL approval memoranda and the associated NSLs contain consistent information and certifications.

Three additional recommendations are designed to reinforce the FBI's obligation to provide timely reports of possible intelligence violations, ensure that these reports detail the precise remedial measures employed to handle unauthorized NSL-derived information, and provide case agents and supervisors with examples of common errors in the use of NSLs. We address the last recommendation to the Department regarding the NSL Working Group's proposal to the Attorney General.

Finally, as noted above, we are continuing our investigation of the FBI's previous use of exigent letters, the blanket NSLs, and other improper NSLs and requests for telephone records. The findings and recommendations in this NSL report should be considered in conjunction with the findings of that forthcoming report.

CHAPTER TWO:
STATUS OF THE FBI'S AND DOJ'S CORRECTIVE ACTIONS IN RESPONSE TO THE OIG'S FIRST NSL REPORT

In our first NSL report, we made 11 recommendations to the FBI to help improve its use and oversight of national security letters. In a letter to the OIG dated March 6, 2007, that was included as an appendix to that report, the FBI stated that it agreed with each of the recommendations and would work with the Department's National Security Division (NSD) and the Office of the Chief Privacy and Civil Liberties Officer (Privacy Officer) to implement the recommended reforms.[7]

In May 2007 and September 2007, the FBI provided memoranda to the OIG describing the status of the FBI's efforts to implement these recommendations. The FBI Inspection Division and the FBI Office of the General Counsel (FBI OGC) have also provided updates to the OIG on the FBI's progress in implementing specific recommendations. Further, the Department's NSD has implemented additional measures to address the serious concerns we uncovered regarding the use of national security letters.

In this chapter, we assess the progress of the FBI's and the Department's efforts to address the problems that our first report found with the use of national security letters. To assess these efforts, we analyzed the FBI's memoranda describing the status of its corrective actions; interviewed FBI officials from the OGC and Inspection Division; interviewed other senior FBI officials, including the FBI Director and Deputy Director; and interviewed field personnel responsible for issuing and reviewing NSLs such as the Special Agents in Charge (SAC), Chief Division Counsels (CDC), Supervisory Special Agents, and Special Agents. In addition, to assess the Department's actions, we reviewed all new NSL-related guidance issued by the FBI to the field and Headquarters divisions since our first report was issued, reviewed the types of NSL training provided and to whom it was provided, and observed a demonstration of the new data system that was designed to manage and track NSLs.

In Section I of this chapter, we provide an overview of the FBI's and the Department's efforts to implement our recommendations and the additional steps it has taken to promote compliance with the NSL statutes, applicable Attorney General Guidelines, and internal FBI policies governing the use of NSLs. In Section II, after listing each of our 11 recommendations and the background for each, we summarize the FBI's responses to the

[7] See NSL I, Unclassified Appendix.

recommendations and analyze the FBI's efforts to date to implement the recommendations.

In Section III of this chapter, we describe other corrective measures implemented in 2007 by the FBI, the Department's NSD, and the Privacy Officer. We also describe the FBI's creation of a new Office of Integrity and Compliance (OIC). In addition, we assess a proposal from a working group led by the Privacy Officer that relates to the retention of NSL-derived information.

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

In the year since the OIG issued its first report on NSLs, the FBI and other Department components have implemented a series of measures designed to promote stricter compliance with NSL statutes, Attorney General Guidelines, and internal FBI policies governing use of NSL authorities. Some of these measures directly respond to the OIG's specific recommendations, while others were additional measures proposed or implemented by the FBI, NSD, or the Attorney General.

In this follow-up review, we examined the FBI's and the Department's actions, as of December 2007, in response to the OIG's recommendations. Some of these actions are one-time measures (such as the FBI's statistical reviews of NSLs issued by field and Headquarters divisions in 2003 through 2006 and the FBI's review of NSLs issued in counterintelligence investigations pursuant to the *Fair Credit Reporting Act* (FCRA) from 2002 through 2006). Others are longer-term actions that require sustained commitment by the FBI's senior leadership, attorneys, CDCs, and other FBI and Department personnel to be fully implemented.

Our recommendations in our first NSL report fell into four broad categories.

- Four recommendations (numbers 1, 2, 3, and 6) focused on enhancements in FBI recordkeeping and information technology supporting the use of NSLs. These recommendations were intended to improve the FBI's ability to capture accurate, complete, and timely information on NSLs for congressional and public reporting; to render NSLs subject to effective internal and external reviews; and to identify when NSL-derived information was used in analytical intelligence products or provided to law enforcement authorities for use in criminal proceedings.
- Three recommendations (numbers 4, 7, and 8) addressed the need for additional guidance and training to ensure that FBI personnel use NSLs in accordance with pertinent authorities, to

reduce or eliminate common mistakes in the issuance of NSLs, to clarify distinctions among the different NSL statutes, to identify possible Intelligence Oversight Board (IOB) violations arising from the use of NSLs, and to eliminate the use of exigent letters.

- Three recommendations (numbers 9, 10, and 11) focused on the role of attorneys in the FBI OGC and the CDCs in providing advice about NSLs. These recommendations were designed to promote better oversight by the FBI OGC's National Security Law Branch (NSLB) at FBI Headquarters, close and independent review of NSLs by CDCs, and clear guidance about the use and sequencing of NSLs in accordance with the requirement in the Attorney General Guidelines to use the "least intrusive collection techniques feasible."
- One recommendation (number 5) suggested that the FBI consider seeking a legislative amendment to the *Electronic Communications Privacy Act* (ECPA) to clarify the information the FBI is entitled to obtain through ECPA NSLs.

OIG Findings on the FBI's and Department's Corrective Actions

Our review found that the FBI and the Department have made significant progress in implementing our recommendations and in adopting other corrective actions to address problems we uncovered in the use of national security letters. We also found that the FBI has devoted significant energy, time, and 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, there are additional steps that the FBI is still considering and needs to take, and we believe that ensuring full compliance will require the continual attention, vigilance, and reinforcement by the FBI and the Department. We also believe it is too soon to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with the use of NSLs that we and the FBI have identified.

It is important to first note that the FBI's leadership has made it a top priority for the FBI to correct the serious deficiencies in the use of NSLs. In our interviews with Director Mueller, Deputy Director Pistole, and General Counsel Caproni, it was clear to us that they appreciated the importance of this issue, the significance of the problems that we had uncovered, and the critical need to correct these problems.

For example, Director Mueller said he believes that the FBI's shortcomings in complying with NSL authorities resulted from the FBI's previous lack of focus on the procedures necessary to ensure that all legal

requirements were satisfied. He attributed the problems to several factors, including inadequate infrastructure at FBI Headquarters to ensure that all legal requirements were followed, organizational "stove piping" under which FBI personnel did not fully communicate across division lines, rotation of FBI middle management so that they did not always "take ownership" of problems they encountered, the significant pressure to respond to any terrorist threat, and inadequate staffing in the FBI's Counterterrorism Division (CTD) in the period following the September 11 attacks.

Director Mueller also emphasized his commitment to address problems in the FBI's use of NSLs, and, as one example, pointed to the establishment of the FBI's OIC (discussed in Section III of this chapter). He stated that he believes this office will assist him and other members of the FBI's senior leadership in identifying and addressing areas of weakness as well as other compliance issues. He also stated that he believes that he has been successful in driving down through the organization the necessity of adhering to NSL authorities and that SACs are "on board" with the NSL compliance and training initiatives and are communicating this message throughout the ranks of the FBI.

FBI Deputy Director Pistole similarly told the OIG that the FBI is devoting significant time and attention to ensuring that SACs understand the substantive legal requirements for NSLs. One of the venues he said he is using to reinforce these requirements is the Strategy Performance Sessions he chairs each quarter via teleconference with the SACs in the FBI's 56 field offices. Each of the ten sessions is held with approximately 6 SACs each and lasts approximately 90 minutes. The second quarter 2007 sessions, which also were attended by the FBI General Counsel, were called, "Preserve Civil Liberties." These sessions focused on the OIG's findings in our first NSL report and the FBI's findings on NSL compliance problems identified in its field office reviews (described in Chapter Three of this report).

Deputy Director Pistole also stated that he is stressing NSL compliance in conjunction with mid-year progress reviews and annual performance appraisals of SACs. During these reviews, he asks the SACs individually what they are doing to ensure compliance with NSL requirements and requires them to cite examples. As the rating official for all SACs, he said that he expects SACs to know the substantive legal requirements for NSLs and regularly stresses in their progress reviews that they cannot assume that their personnel are following FBI guidance on NSLs.

FBI General Counsel Caproni stated that she has devoted significant time and attention to addressing the OIG's recommendations and implementing other measures to improve NSL compliance. Following

release of the OIG's report, Caproni held a conference call in March 2007 with all CDCs to review the OIG's most significant findings, describe the FBI's response, and underscore the role of CDCs in reviewing and approving NSLs and ensuring that any unauthorized information obtained from NSLs is handled appropriately. She also discussed these issues at the CDC conference in July 2007 and the SAC conference in October 2007. Caproni emphasized at the CDC conference that it is "clearly and unequivocally" the duty of CDCs to review predication for NSLs.

Caproni also noted that the FBI OGC had issued or was preparing to issue additional guidance on NSLs based on the OIG's findings and the additional findings developed from the FBI's reviews in 2007. Among the new guidance issued were memoranda directing FBI case agents to review NSL-derived records prior to uploading them into FBI databases to ensure that they correspond to the NSLs and have not generated unauthorized information; prohibiting the use of exigent letters; reiterating the distinctions between the NSL authorities in the FCRA; clarifying the role of CDCs in conducting independent reviews of NSLs; and describing procedures for redacting NSL-derived information that is beyond the scope of the NSL to prevent unauthorized dissemination. In June 2007, the FBI OGC issued a comprehensive 24-page memorandum on the use of NSL authorities that covered these topics.[8]

Caproni also stated that the FBI OGC has devoted additional resources to support the NSL-related activities of FBI Headquarters divisions, including the assignment of additional NSLB attorneys to either be co-located with or to support all the CTD sections. She believes that these additional resources will assist the FBI OGC in identifying and

---

[8] These memoranda are described in more detail in Section II of this chapter in conjunction with our analysis of the FBI's implementation of recommendations 4, 7, 8, and 10.

Caproni also noted that in August 2007, the FBI OGC requested a legal opinion from the Department's Office of Legal Counsel (OLC) on three issues that arose in the course of the FBI's 2007 NSL reviews. The three questions were: (1) whether, in response to *Electronic Communication Privacy Act* (ECPA) NSLs, the FBI may obtain Social Security Numbers, dates of birth, and other information used by the communication provider to identify or maintain a profile of a customer or subscriber; (2) whether the term "toll billing records information" in the ECPA NSL statute includes records of incoming/outgoing calls upon which a fee could be assessed regardless of whether a fee is actually assessed and regardless of whether the information must be culled from aggregate data; and (3) whether the government may obtain information verbally regarding the existence of an account in connection with a given telephone number or person from an electronic communication service provider without additional legal process. As of February 11, 2008, OLC had not provided its opinion on these questions. Caproni stated that once OLC issues its opinion, the FBI OGC will determine what steps it must take to address the appropriateness of retaining NSL-derived information in the categories covered by the opinion.

avoiding potential problems before they occur. In March 2007, Caproni also ordered all NSLB attorneys to provide live training any time they visit a field office.

In addition to the FBI's efforts to address the OIG's recommendations, the Department's NSD has implemented additional measures to promote better compliance with NSL authorities and to address the privacy issues raised by our first report. For example, in 2007 the NSD began national security reviews to examine whether the FBI is using various intelligence techniques, including NSLs, in accordance with applicable laws, guidelines, and policies.

Also, the Privacy Officer convened a working group to examine how NSL-derived information is used and retained by the FBI, with special emphasis on the protection of privacy interests, and sent a proposal to the Attorney General for review on minimization procedures with respect to NSL-derived data.

Based on our review, we believe the FBI and the Department have taken significant steps to address the findings of the OIG's first report on NSLs and have made significant progress in implementing corrective actions. However, we also believe it is too soon to state with full confidence whether the steps the FBI and the Department have taken will eliminate fully the problems we identified in our first report on NSLs. Some measures, such as the FBI's new NSL data system and the OIC are positive steps but are not fully implemented or tested. Other measures, such as the NSD's reviews and the recent FBI OGC guidance on the responsibility of case agents to ensure that information obtained from NSLs has not generated unauthorized collections, have not been in place long enough to gauge their effectiveness.

Yet, despite the multiple challenges facing the FBI to eliminate fully problems in the use of NSLs, we believe the FBI and the Department have evidenced a commitment to correcting the problems we found in our first NSL report and have made significant progress in addressing the need to improve compliance in the FBI's use of NSLs.

In the next section of this chapter, we discuss in greater detail the specific steps that have been taken or are planned to address each of the OIG's 11 recommendations. After that, we examine other initiatives implemented by the FBI and the Department regarding NSL use.

II. Status of the FBI's Implementation of the OIG's Recommendations in Our First NSL Report

We set forth below each of our recommendations in our first NSL report, describe the background for the recommendations, summarize the actions taken by the FBI to date to address the recommendations, and provide our analysis.

Recommendation No. 1

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

Background: In our first NSL report, we found that the FBI did not have policies requiring the retention of signed copies of NSLs or the uploading of NSLs into the FBI's principal investigative database, the Automated Case Support (ACS) system. This meant that the FBI did not have a reliable audit trail tracking the issuance of NSLs, which prevented internal and external reviews of compliance with NSL statutes, applicable Attorney General Guidelines, and internal FBI policies governing the use of NSLs.

FBI Actions Taken to Address the Recommendation: The FBI issued three communications to field and Headquarters divisions to address this recommendation. On March 6, 2007, the FBI OGC sent an e-mail message to all CDCs and SACs directing that copies of signed NSLs be maintained both in the investigative file and a field office "drop" file so that all NSLs issued by each field and Headquarters division are maintained and can be located in one place. This was superseded by the FBI Records Management Division's memorandum dated March 9, 2007, requiring that signed copies of NSLs be retained in the relevant investigative file by the issuing division. This requirement is reiterated in the FBI OGC's Comprehensive Guidance on National Security Letters (Comprehensive Guidance EC) issued on June 1, 2007 (also discussed in connection with Recommendation Nos. 3,4, and 8 through 11).

OIG Analysis: We believe that the steps taken by the FBI will help ensure that copies of all issued NSLs are retained in a file created by field and Headquarters divisions. Maintaining signed copies of the NSLs in the pertinent investigative files should ensure that all NSLs issued by a field office or Headquarters division are collected in one location and are available for internal or external audits or reviews.

Recommendation No. 2

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

Background: In our first NSL report, we found the FBI OGC NSL tracking database (OGC database) did not contain accurate and complete information about NSL requests. This occurred because of flaws and structural problems in the database. In addition, since the FBI relied upon the OGC database in preparing the Department's semiannual classified reports to Congress, the flaws and structural problems in the database affected the accuracy of the Department's reports to Congress. For example, in the 77 case files we examined in 4 field offices in connection with our first NSL report, we found that for the period 2003 through 2005, the OGC database underreported the total number of NSLs and NSL requests by 17 percent and 22 percent, respectively.

We also identified circumstances in which certain data fields in the OGC database were left blank, had typographical errors or other erroneous entries, or contained default settings – all of which resulted in errors or understatements in reporting to Congress on NSLs. We also found that delays by FBI field and Headquarters personnel in entering data into the ACS system contributed to additional discrepancies in the data reported to Congress, including the failure to report almost 4,600 NSL requests for the period 2003 through 2005. Other structural problems or flaws in the database resulted in discrepancies affecting the Department's reporting of the total number of NSL requests, the total number of "investigations of different U.S. persons", and the total number of "investigations of different non-U.S. persons" that were reported to Congress over the 3-year period.

In light of these flaws and structural problems with the OGC database, we recommended that the FBI improve its database to ensure the collection of timely, complete, and accurate data on NSL usage for purposes of congressional and public reporting and to facilitate internal and external audits or reviews.

FBI Actions Taken to Address the Recommendation: The FBI OGC issued an EC dated March 19, 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. According to the EC, any discrepancies identified by the FBI OGC are being reconciled and will be used to improve guidance and training on NSL reporting. The

FBI told the OIG that it will continue requiring these monthly counts and reconciliations until the new database for tracking NSL data is implemented. This database, discussed below, known as the NSL sub-system to the Foreign Intelligence Surveillance Act (FISA) Management System (NSL data system), has replaced the OGC database. While the new data system does not correct historical information, it is designed to improve the accuracy of NSL data in the future.

FBI OGC personnel reported that the FISA Unit of the FBI OGC's NSLB developed the NSL data system to facilitate the approval and issuance of NSLs and support data collection for congressional and public reporting. The NSL data system prompts the drafter of an NSL to enter information about the subject, the predication for the NSL, the type of NSL, the NSL recipients, and the specific information sought by the NSL (such as telephone numbers or e-mail addresses). The NSL data system will route the NSL request through the required levels of review and approval similar to the manner in which applications for use of FISA authorities are routed in the FBI. Upon completion of all approvals, the NSL data system will generate the approval EC and the NSLs for signature by the field or Headquarters approving officials. As a result, the accuracy of NSLs and the efficiency of issuing NSLs should improve, and there also should be fewer discrepancies between the approval ECs and the NSLs. The FBI established an automatic link between the NSL data system and the ACS system that facilitates automatic uploading of approval ECs and NSLs into the ACS system. In addition, FBI OGC personnel said that all information necessary to generate the Department's congressional and public reporting will be collected as part of the new NSL data system. The FBI informed us that on January 1, 2008, this system was deployed throughout the FBI.

The Records Management Division's March 9, 2007, directive noted previously also mandated that NSLs be uploaded into the ACS system as an NSL "Document Type" to facilitate recordkeeping and reporting. As a result, NSLs issued after March 9, 2007, can now be sorted and counted by field office in the ACS system, which will help verify the accuracy of information used in the Department's congressional and public reports on NSLs and will assist in facilitating internal and external NSL reviews.[9]

In addition, in an attempt to correct deficiencies in the existing OGC database, the NSLB has modified the database so that FBI personnel making entries about NSLs must complete all fields required for

---

[9] The "Document Types" are Telephone Subscriber Information; Telephone Toll Records; E-Mail Subscriber Records; E-Mail Transactional Records; Financial Records, *Right to Financial Privacy Act* (RFPA) § 3414 (a)(5); Financial Institution Listings, FCRA; Consumer Identifying Information; and Full Credit Report.

congressional and public reporting. The FBI also changed the default setting in the OGC database on the status of the NSL target from "non-U.S. person" to "U.S. person" and changed the default number of NSL requests from "0" to "1." The FBI told us that it believes these changes should reduce errors caused by the previous default settings.

The FBI OGC assigned additional personnel to enter data into the OGC database and conducted training for all personnel who entered NSL data to ensure they understand the data being entered and recognized when incorrect data had been provided. These measures were designed to improve the old database before the new NSL data system was implemented. Now, all reporting of NSLs is done through the new system.

OIG Analysis: We believe that the steps taken by the FBI to create a central database for generating and approving NSLs and for collecting data pertinent to congressional and public reporting on NSL usage should improve the collection of timely, complete, and accurate data on NSLs. This new NSL data system will enable field agents to insert case-specific information into a standardized NSL request form, automatically track the progress of each NSL, identify delays in the process, send automatic reminders to advance the review and approval process, and facilitate the transmission of NSL documents among participants in the NSL approval process.

Now that the NSL data system is fully operational, it should eliminate the need for FBI OGC personnel to manually re-enter NSL data into the antiquated OGC database after the information has been uploaded into the ACS system by field and Headquarters personnel. Using the new data system, FBI field personnel will need to enter NSL data only once – when the NSL is created – because the data system will automatically upload the approval EC and NSL into the ACS system. The FBI stated that all the information necessary to produce required congressional reports on NSLs will be collected as part of this process, which should improve the timely, complete, and accurate collection of NSL data.

The FBI also stated that the NSL data system contains controls to minimize the risk of data entry errors, such as setting the default to U.S. person, prohibiting an entry of "0" for the number of requests, and preventing the use of consumer full credit reports in counterintelligence cases. However, the OIG disagrees that changing the default setting status from a "non-U.S. person" to a "U.S. person" is the best way to ensure accurate data entry. As we noted in our first NSL report, from 2003 through 2005 the OGC database contained a default setting of "non-U.S. person" for the investigative subject of NSL requests for *Right to Financial Privacy Act* (RFPA) and ECPA toll billing/electronic communication transaction records. As a result, known or presumed U.S. persons could be misidentified if the

default setting was not corrected (from "non-U.S. person" to "U.S. person") during data entry. This resulted in an understatement of the number of investigations of U.S. persons who were the targets of NSLs. The OIG believes that an error is just as likely to occur if the default is changed to "U.S. person" because personnel entering the data may fail to correct the default setting when the target of the investigation is a "non-U.S. person." We believe the appropriate way to minimize the risk of error would be to create a blank mandatory field and require FBI personnel to make an affirmative selection before the data system allows the user to proceed to the next entry.

Similarly, as described in our first NSL report, the OGC database was programmed to provide a default setting of "0" for the number of NSL requests. Since every NSL generates at least one NSL request, a "0" entry for NSL requests is erroneous. However, since one NSL can generate more than one request, FBI personnel may fail to correct the new default "1" setting just as they previously failed to correct the previous default "0" setting." According to the FBI, the new NSL data system corrects this deficiency because it assigns the number of NSL requests automatically.

We believe that the FBI's decision to assign additional NSLB personnel to enter data into the database and provide additional training for these personnel should help reduce the frequency of data entry errors. However, we also believe that the FBI OGC should require periodic reviews of a sample of NSLs in the new NSL data system to ensure that the training provided is successfully applied in practice and has reduced or eliminated data entry errors.

The OIG also notes that the NSL data system does not capture the date when the SAC (or other approving official) signs the NSL; rather, it includes the date that the SAC electronically certifies approval of the EC and NSL. Until the FBI implements electronic signature capability, this may create a possible variance between the two dates.

Recommendation No. 3

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

Background: We determined in our first NSL report that the OGC database did not include data on whether the target of the NSL is the subject of the underlying investigation or another individual. The target of an NSL is frequently not the same person as the subject of the underlying investigation. Since the database did not distinguish between the target of the NSL and subject of the investigation, the FBI did not know and was

unable to estimate the number of NSL requests relating to persons who are not investigative subjects. In light of the Patriot Act's expansion of the FBI's authority to collect information on individuals who are not subjects of its investigations, we recommended that the OGC database be modified to capture this information from NSL approval ECs so that the information is subject to internal and external oversight.

FBI Actions Taken to Address the Recommendation: The new NSL data system will prompt the user to enter information about the subject, the predication for the NSL, the type of NSL, the NSL recipient, and specific targets of the NSL, including targets other than the subject of the investigation.

In 2006, the FBI modified its NSL guidance to require, with the exception of NSLs seeking subscriber information, that agents indicate in the NSL approval EC whether the request is for a person other than the subject of the investigation or in addition to that subject and to state the U.S. person or non-U.S. person status of those individuals.[10] That guidance was reiterated in the Comprehensive Guidance EC issued by the FBI OGC in June 2007.

OIG Analysis: Our review indicates that the steps taken by the FBI will help ensure that the new NSL data system contains accurate data about individuals who are not investigative subjects but are the targets of NSL requests. We reviewed a demonstration of the NSL data system, which indicated that, when fully implemented, the new data system should satisfy our recommendation by capturing data on the U.S. person/non-U.S. person status of targets of NSLs, not just the status of the investigative subjects.

Recommendation No. 4

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

---

[10] There is no statutory requirement in the ECPA to report the U.S. person status of NSL requests for subscriber information. In many cases, the identity of the subscriber is unknown.

Background: Our first NSL report noted that the majority of the possible intelligence violations that were self-reported by FBI personnel to the FBI OGC by field offices, 22 of 26, arose from FBI errors. Most of these involved typographical errors or the case agent's good faith but erroneous belief that the information requested related to an investigative subject. Moreover, many NSL-related possible intelligence violations throughout the FBI were not identified or reported by FBI personnel.

Some of the possible intelligence violations we identified resulted from typographical errors in the telephone number or e-mail address in the NSLs. We also determined that the FBI entered unauthorized information in an FBI database because agents and intelligence analysts did not verify that the information supplied by the NSL recipients matched the information requested in the NSLs. Additionally, we found that some FBI personnel were confused about the two NSL authorities available under FCRA NSL statutes and, as a result, either requested or obtained unauthorized information.

We also identified two circumstances in which the FBI relied exclusively on control files rather than investigative files to initiate approval for NSLs in violation of internal FBI policy. In one instance, the FBI issued at least 300 NSLs in connection with a classified special project overseen by FBI Headquarters. The second instance involved the issuance of six NSLs by the Electronic Surveillance Operations and Sharing Unit in the Counterterrorism Division. In addition to violating FBI policy, when NSLs are issued exclusively from control files it is difficult to determine if the statutory and Attorney General's Guidelines requirements for issuing NSLs have been satisfied.

Unless the errors in the use of NSLs are identified by the FBI promptly and any improperly obtained information is sequestered or returned, unauthorized information obtained in response to improper NSLs may result in additional problems. In some instances, agents and analysts upload digital responses to NSLs into the ACS system and the Investigative Data Warehouse, which makes the data available to other agents, Headquarters personnel, and other law enforcement and intelligence agencies. Accordingly, we recommended that the FBI consider issuing additional guidance that would assist FBI personnel in identifying possible intelligence violations arising from these types of errors.

FBI Actions Taken to Address the Recommendation: **4(a) measures to reduce or eliminate typographical and other errors in national security:** In a Comprehensive Guidance EC, the FBI General Counsel mandated that the model NSL approval ECs and model NSLs posted on the NSLB website be used by FBI personnel when drafting the NSLs. The FBI believes that mandatory use of these models will help reduce

typographical errors in NSLs and approval ECs. The FBI also provided new NSL training to field and Headquarters personnel that emphasized the potential for collection of unauthorized information due to typographical errors and the need to ensure that information is appropriately requested. In addition, as described in Chapter Three of this report, several reviews of the FBI's use of NSL authorities conducted in 2007 by the FBI's Inspection Division and national security reviews conducted by the NSD will assist the FBI in developing additional guidance to reduce these and other types of errors.

OIG Analysis: **4(a)** The OIG believes that the steps taken by the FBI will help reduce typographical and other errors in NSLs so that the FBI does not collect unauthorized information.

We believe that mandating the use of the model NSL approval ECs and model NSLs in conjunction with the new NSL data system (in which data elements such as case numbers, type of NSL, subject and target names, and telephone numbers must be typed only once) should help to reduce typographical and other data entry errors. Once typed, the information becomes part of the electronically generated approval EC and accompanying NSL. These steps will avoid the electronic "cutting and pasting" that created errors as we noted in our first NSL report. However, case agents and supervisors will still need to verify that the initial data entries are made correctly. To verify this, we recommend that the information in the NSL be checked by the case agent or the supervisor against any serialized source document to verify that the data extracted from the source document and used in the NSL (such as the telephone number or e-mail address) is accurately entered.[11] This would enable FBI personnel and internal and external auditors to compare the data in the source document with the particulars described in the NSL to ensure consistency and accuracy.

The OIG also believes that periodic training of FBI personnel responsible for generating, reviewing, and approving NSLs that emphasizes the need to ensure that information is appropriately requested in NSLs and identifies the potential for unauthorized collections due to typographical and other errors is essential to the success of these corrective actions.

FBI Actions Taken to Address the Recommendation: **4(b) best practices for identifying the receipt of unauthorized information in the response to national security letters due to third party errors:** On

[11] Under FBI internal procedures, each document that is placed in an investigative file must be numbered in sequence. This number is known as the serial number, and the document is known as the serial. Federal Bureau of Investigation, Manual of Administrative Operations and Procedures, 2-4.1.1.

January 3, 2007, the FBI OGC issued a memorandum entitled, Legal Advice and Opinions; Uploading of NSL Return Information. The memorandum directed that information obtained in response to NSLs be reviewed before it is uploaded into Telephone Applications and other FBI databases to ensure that the information is responsive to the NSL request and that there has been no unauthorized collection. The Comprehensive Guidance EC issued on June 1, 2007, reiterated this policy and states that any improper information obtained in response to NSLs may not be retained or uploaded into any FBI database and must immediately be sequestered. It further stated that a report to the FBI OGC of a potential intelligence violation must be prepared by the case agent. The January 3 memorandum also stated that when the NSLB adjudicates the matter, it is to confirm whether the information is relevant. If the information is not relevant, the NSLB will direct that the information either be returned or destroyed. If unauthorized information is collected that is relevant to the investigation, the memorandum directs that it be sequestered and not uploaded into any FBI database or utilized in any manner until another NSL has been issued to address the overproduction.

The Comprehensive Guidance EC includes as an attachment an NSL Review Checklist for use by personnel who review or upload NSL-derived information. The checklist has a check box indicating that the case agent has confirmed that the information is relevant and there has not been an unauthorized collection. There also is a check box indicating that if the information is not relevant to the investigation the user has contacted the CDC or the NSLB for advice on how to proceed with a potential IOB report and that the CDC will sequester the information and determine the appropriate action.

The Comprehensive Guidance EC also differentiated between two categories of unauthorized collections: production of information not relevant to the investigation and "overproduction" of information that was not requested by the NSL but is relevant to the investigation. Information not relevant to the investigation would include data on a telephone number other than the telephone number listed in the NSL due to a typographical error in the NSL. In addition, an NSL recipient may generate unauthorized collections by providing information on the subscriber associated with the telephone number referenced in the NSL for a time period greater than was requested. The Comprehensive Guidance EC directs that supervisors are required to monitor compliance with this policy, recommending that during quarterly file reviews squad supervisors conduct spot checks of information obtained in response to NSLs to ensure that case agents are following these procedures.

The FBI OGC also issued a memorandum on April 4, 2007, regarding procedures for redacting information obtained in response to, but beyond

the scope of, an NSL and for disseminating the information to case agents while awaiting adjudication of the potential intelligence violation. The method of redaction is left to the discretion of the CDC. However, the procedures require that no matter what method is used, the redacted information should not be visible or accessible, should not be uploaded into any FBI database, and should remain sequestered with the CDC.[12]

New NSL training also addresses the need to review NSL-derived information prior to uploading it to FBI databases. In addition, we were informed that the FBI OGC and the NSLB are reviewing the findings of the Inspection Division's 2007 review of NSLs to determine if additional measures or training would improve compliance on the handling of unauthorized information obtained in response to NSLs.

OIG Analysis: **4(b)** We believe that the steps thus far taken by the FBI will assist FBI personnel in identifying possible intelligence violations arising from use of NSL authorities. The FBI OGC guidance memoranda dated January 3, 2007, and April 4, 2007, and the Comprehensive Guidance EC provide specific instructions for handling unauthorized records obtained in response to NSLs and direct that such records not be uploaded into any FBI databases.

The new NSL data system also requires case agents reviewing NSL-derived information to identify the receipt of any unauthorized information. When case agents receive records in response to NSLs, they must complete several steps, including entering an electronic certification stating that the responsive records have been reviewed for unauthorized collection. The data system has a comment field that must be completed if an unauthorized collection occurs. If the person entering data does not complete all required tasks, the data system sends electronic reminders until all required entries are made.

In its response to our recommendations that address potential errors by the FBI or NSL recipients, the FBI noted its implementation of new training, issuance of new guidance, and development of the new NSL data system. While we believe these measures are important, we also believe the FBI needs to proactively and regularly scrutinize national security investigations and the use of NSLs. In light of the FBI's increasing reliance on NSLs as a primary investigative technique employed in both terrorism and espionage investigations (discussed in Chapter Five of this report), the FBI should examine the preparation of NSL-related documents and the

[12] When a portion of NSL-derived information is redacted by a "strike-though" or by "blacking out" using a black marker or other similar marking device, the information must not be legible through the blackened/redacted portion.

handling of NSL-derived information with periodic reviews and inspections. Any recurring problems that suggest continuing confusion or uncertainty about the proper use of NSLs, or inadequate field supervision and review, should be promptly discussed with FBI attorneys and addressed. We also believe that the FBI OGC should establish mechanisms for spot checking entries into the new NSL data system using resources available from the FBI Inspection Division and the FBI's new OIC. Moreover, FBI personnel authorized to request information pursuant to the NSL authorities must know that the use of these authorities imposes requirements and responsibilities for which they will be held accountable.

FBI Actions Taken to Address the Recommendation: **4(c) clarifying the distinctions between the two NSL authorities in the *Fair Credit Reporting Act*:** A memorandum dated March 5, 2007, issued to all field offices and the Counterintelligence Division by the FBI National Security Branch (NSB), clarified the distinction between 15 U.S.C. § 1681u and 15 U.S.C. § 1681v of the FCRA and mandated a review of NSLs issued under the FCRA. The distinction between the two NSL authorities also is highlighted in the Comprehensive Guidance EC.

As we describe in Chapter Three of this report, on March 5, 2007, the FBI's Executive Assistant Director for the NSB also directed all 56 field offices to review all NSLs issued pursuant to the FCRA in counterintelligence case files from 2002 through 2006. The purpose of the review was to determine if any of these NSLs requested consumer full credit reports in violation of 15 U.S.C. § 1681v or resulted in the improper collection of such reports in response to NSL requests for limited credit information pursuant to 15 U.S.C. § 1681u. The directive stated that all such incidents must be reported to the FBI OGC as potential intelligence violations regardless of whether the information was requested by the FBI or erroneously produced by the credit reporting agency. The memorandum directed that any improperly obtained consumer full credit reports be removed from the files and that any possible intelligence violations identified through the review be reported. We describe the results of the FCRA review in Chapter Three of this report. In sum, the review showed that the FBI issued at least 33 NSLs seeking consumer full credit reports in counterintelligence cases in violation of the FCRA NSL statute and internal FBI policy. In 29 of these 33 matters, the FBI obtained the consumer full credit reports. The unauthorized information was sequestered in 23 instances, returned to the third party provider in 1 instance, and in 5 instances the ECs did not state what was done with the information.

The FBI General Counsel also provided training at the counterintelligence conferences for SACs in January and February 2007 regarding NSLs, the SACs' responsibilities prior to authorizing NSLs, and the

fact that an NSL for a consumer full credit report is not authorized in a counterintelligence investigation absent an international terrorism nexus.

In addition, new NSL training addresses the distinction between the two FCRA NSL authorities and emphasizes the need to identify a nexus to international terrorism before generating an NSL pursuant to 15 U.S.C. § 1681v in a counterintelligence investigation.

OIG Analysis: **4(c)** The FBI's FCRA review revealed that 20 percent of the FBI's field offices (11 of 56) issued a total of 33 improper FCRAv NSLs during 2002 through 2006, the 5-year period covered by the review. In 29 of these instances, the FBI improperly obtained consumer full credit reports. The review determined that only two of these matters had previously been reported to the FBI OGC pursuant to the mandatory self-reporting requirement. The review also showed that 64 percent of the FBI's field offices (35 of 56) issued a total of 233 NSLs seeking limited credit information pursuant to 15 U.S.C. § 1681u during the review period, in response to which the credit reporting agencies improperly produced consumer full credit reports. Only 6 of the 233 unauthorized collections had previously been reported to the FBI OGC pursuant to the mandatory self-reporting requirement. Thus, only 6 percent of the improper requests and 3 percent of the unauthorized collections were self-reported to the FBI OGC.

The results of the FBI's review demonstrated continued confusion or inadequate knowledge about the statutory requirements for FCRA NSLs among case agents, supervisors, and CDCs throughout 2006. Moreover, the results demonstrated the ineffectiveness of the FBI's mandatory self-reporting requirements. The case agents, their supervisors, their attorneys, and the SACs did not recognize that they had made improper requests under the FCRA. Similarly, the case agents and analysts who reviewed the responsive records did not recognize the receipt of the unauthorized collections.

The OIG believes that the steps thus far taken by the FBI will help clarify the distinctions between the two types of FCRA NSLs. In addition, the new NSL data system is programmed so that FBI personnel cannot generate an NSL request for a consumer full credit report from a counterintelligence case file. Also, as demonstrated in the new NSL data system training module, when the statute under which the records are requested is selected, the language of the statute appears in a textbox. The text of the NSL statute informs the requester what records the FBI is authorized to obtain under each NSL statute. The results of the FBI's review of FCRA NSLs will also assist the FBI in developing further training to assist agents and supervisors in distinguishing the two types of FCRA NSLs.

However, successful implementation of this recommendation will require review by case agents, their supervisors, and CDCs and Headquarters attorneys of all FCRAv NSLs to verify the required nexus to international terrorism exists. To identify any unauthorized collection of records obtained in response to any type of FCRA NSL, the responsive records must be carefully and consistently reviewed upon receipt. Case agents and their supervisors must be vigilant to ensure that any unauthorized collections are promptly identified and reported in accordance with FBI policies.

FBI Actions Taken to Address the Recommendation: **4(d) reinforcing internal FBI policy requiring that NSLs must be issued from investigative files, not from control files:** In an EC dated February 23, 2007, the FBI OGC mandates that NSLs be issued from open investigative files and that the NSL approval EC must not refer solely to a control file number. The Comprehensive Guidance EC also prohibits NSLs from being issued solely from a control file. The EC notes that absent reference to an authorized investigation it is difficult for the FBI to ensure for purposes of congressional reporting and auditing that the requirements of the NSL statute are met.

The new NSL data system incorporates the requirements of the February 23, 2007, EC in its programming by precluding case agents from generating an NSL solely from a control file.

OIG Analysis: **4(d)** The steps taken by the FBI reinforce internal policy requiring that NSLs be issued only from investigative files, not solely from control files. The clear guidance contained in the February 23, 2007, EC mandates that NSLs be issued from open investigative cases and further states that: (1) the NSL approval EC must refer to the investigative case file or sub-file number of the investigation to which the NSL relates; (2) NSLs should not be issued under control file numbers; and (3) investigative activity requiring an open investigation, such as issuing NSLs, may not be conducted solely from a control file. This policy was reiterated in the Comprehensive Guidance EC and also is referenced in the FBI's mandatory NSL training provided for field agents assigned to counterterrorism or counterintelligence squads. Additionally, the new NSL data system will ensure that NSLs are not being requested solely from control or administrative files.

Both the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines) and FBI policy require that an NSL issued in a national security investigation be issued from an open investigative file. Regular monitoring that includes file reviews and periodic reminders will help ensure that NSLs are issued only from open national security investigation case files.

Recommendation No. 5

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

Background: We found in our first NSL report that FBI agents and attorneys frequently had questions regarding the types of records they could obtain when requesting "toll billing records information," a term that is not defined in the ECPA NSL statute. The imprecision of the statutory language and sparse case law generated multiple inquiries by CDCs to NSLB attorneys and confusion on the part of communication service providers who provided different types of information in response to the FBI's ECPA NSLs. Accordingly, we recommended that the FBI consider seeking legislative revision of the ECPA NSL statute to clarify the records the FBI is permitted to obtain and ensure consistent interpretation of the statute.

FBI Action Taken to Address the Recommendation: Based on recommendations from the FBI, the Department has drafted a proposed amendment to clarify the phrase "telephone toll billing records information" in the ECPA. The proposed amendment specifies the types of information the FBI can obtain pursuant to the ECPA NSL statute. The proposed amendment was cleared by the Office of Management and Budget and was sent to Congress on July 13, 2007.[13] The proposed amendment would authorize 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.

[13] The FBI OGC had no additional information on the status of the proposed legislation as of February 2008.

OIG Analysis: The OIG agrees that, if enacted, the proposed amendment to the ECPA NSL statute would clarify the meaning of the phrase "telephone toll billing records information" 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.

Recommendation No. 6

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

Background: We found in our first NSL report that the FBI generates a variety of analytical intelligence products using information derived from NSLs. These include analyses of communication and financial links between investigative subjects and others, as well as analyses of NSL-derived data in relation to information developed from other intelligence techniques that are stored in other FBI databases, such as the Investigative Data Warehouse. NSL-derived data also is used to generate more formal intelligence products, such as Intelligence Information Reports, Intelligence Assessments, and Intelligence Bulletins. 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 other 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, it is 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 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 can be better tracked in intelligence products and in criminal proceedings.

FBI Actions Taken to Address the Recommendation: At the direction of the Attorney General, in July 2007 the Department's Chief Privacy and Civil Liberties Officer convened a National Security Letter Working Group (NSL Working Group) to examine issues regarding retention of NSL-derived information. The Attorney General directed the NSL Working Group to evaluate how NSL-derived information is used, stored, and disseminated,

with a particular focus on the retention of NSL-derived information.[14] The NSL Working Group considered information provided to it by the FBI about enhancements to the FBI's information technology systems designed to support agents when handling NSL-derived data.[15]

The NSL Working Group concluded that tagging of NSL-derived information was not feasible at the time, but it recommended that the FBI require NSL-derived information to be placed in a specific sub-file of the pertinent investigative file. In a draft memorandum to the Attorney General, dated August 17, 2007 (NSL Working Group August 2007 Draft), the NSL Working Group stated:

> Because the [FBI's] new systems provide for the structured storage of information and NSL information can be segregated in the database, the Working Group concluded that the individual tagging of NSL-derived data did not provide any measurable value for privacy protections at this time. That said, and as explained in more detail in the FBI's proposed directive, ensuring that information derived from NSLs is appropriately labeled as such and tied to a specific NSL does function as a form of tagging. The benefit to privacy of requiring additional tagging, such as through meta-tags, was determined to place an undue burden on the operation of such an important tool.

In brief, the NSL Working Group concluded that additional measures requiring the tagging or labeling of NSL-derived information would "place an undue burden on the operation [of NSLs.]"

As an alternative to tagging, the NSL Working Group recommended that the FBI label all NSL-derived information and place the paper copies or electronic media in an investigative case sub-file specifically designated for NSL-derived information. The NSL Working Group also recommended that the FBI implement minimization procedures for NSL-derived information that were developed by the NSL Working Group. Several of these proposed procedures replicated procedures that the FBI had already developed and implemented in response to the OIG's recommendations in our first NSL report.

---

[14] We provide further analysis of the NSL Working Group's recommendations in Section III of this chapter.

[15] The enhancements included improved processes for: (1) approving and authorizing the issuing of NSLs; (2) reviewing and identifying the responsiveness of records produced pursuant to NSL requests; and (3) ensuring that only NSL-derived information deemed to have investigative value be uploaded into any FBI database.

The NSL Working Group also concluded that existing controls and enhanced guidelines established by the FBI on the acquisition and use of NSL-derived information, if properly followed, could protect privacy interests. The NSL Working Group also stated that the FBI has made significant progress in responding to and rectifying previous concerns about its compliance with statutory and guidelines limitations regarding the use of NSLs, has a better mechanism for tracking its use of NSLs, and is subject to additional oversight through the NSD.

OIG Analysis: As discussed later in this chapter, while we agree that the FBI has made significant progress in addressing our concerns about compliance with NSL authorities, we believe it is too soon to say that the FBI has "rectified" many of the problems we identified in our first NSL report and too early to fully assess whether the new systems and controls will reduce or eliminate these concerns.

The OIG believes that the NSL Working Group's analysis of the tagging issue does not take into consideration the FBI's existing process for labeling NSL-derived information in the ACS system and Telephone Applications database, and whether that process can be adapted–without undue burden and cost to follow NSL-derived information as it travels through other databases and uses. The OIG recommends the FBI and the NSL Working Group give additional consideration to whether the FBI could build upon existing databases without undue burden or cost to label or tag NSL-derived information and to identify when and how often information derived from NSLs is used in analytical intelligence products and provided to law enforcement authorities for use in criminal proceedings.

Recommendation No. 7

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

Background: In our first NSL report, we found that on over 700 occasions the FBI obtained telephone toll billing records or subscriber information from 3 communication service providers without first issuing NSLs or grand jury subpoenas as the statute requires. Instead, the FBI obtained the records with "exigent letters" that were signed by FBI Headquarters Counterterrorism Division personnel who were not authorized to sign NSLs. We also found through interviews of the Counterterrorism Division's Communications Analysis Unit (CAU) personnel and a review of FBI documents that there sometimes were no pending national security investigations associated with the requests at the time the exigent letters were sent. In addition, we found that due to inadequate recordkeeping, the FBI was unable to provide reliable documentation to substantiate that NSLs or other legal process was issued to cover the records obtained in response

to a sample of exigent letters for which we requested such documentation. We also determined that exigent letters sometimes were used in non-emergency circumstances.

We identified additional problems with respect to the CAU's efforts to issue after-the-fact NSLs to cover records obtained from the three communication service providers under contract with the FBI. Among these problems were that the CAU generally: (1) did not inform field division personnel who they asked to issue the NSLs that the information had already been acquired by the FBI and (2) did not consistently provide information establishing predication for the requests necessary to satisfy the ECPA NSL statute, the Attorney General's NSI Guidelines, and internal FBI policy. As a result, the approval ECs issued in connection with the after-the-fact NSLs sometimes violated the Attorney General's NSI guidelines and FBI internal policy.

We concluded that by issuing exigent letters rather than NSLs, the FBI circumvented the requirements of the ECPA NSL statute and violated the Attorney General's NSI Guidelines and internal FBI policy. We were not convinced by the legal justifications offered by FBI attorneys for acquiring the records through exigent letters: (1) to reconcile the strict requirements of the ECPA NSL statute with the FBI's mission to prevent terrorist attacks and (2) that use of exigent letters could be defended as a use of the ECPA's emergency voluntary disclosure authority for acquiring non-content information (18 U.S.C. § 2702(c)(4)). Accordingly, we recommended that the FBI take steps to ensure that the FBI does not issue exigent letters.

FBI Actions Taken to Address the Recommendation: In an EC dated March 1, 2007, the FBI OGC issued a directive prohibiting the use of exigent letters that promise future legal process and reiterated the authorized procedures for obtaining telephone records pursuant to the emergency voluntary disclosure provision of the ECPA, 18 U.S.C. § 2702 (c)(4). The Comprehensive Guidance EC and mandatory NSL training provided to field and Headquarters personnel reiterated the prohibition on the use of exigent letters. In the course of the FBI's review of field and Headquarters NSLs, the Inspection Division included questions designed to ascertain whether exigent letters were used by FBI personnel outside the CAU. The inspectors found no instances in which exigent letters were used by the field in the case files they reviewed.

The FBI OGC also told us it is meeting regularly with the NSD to address issues previously identified by the OIG in our first NSL report. In addition, as discussed further in Recommendation No. 9, NSLB attorneys regularly attend operational meetings of the Headquarters Counterterrorism units that had previously issued exigent letters and Counterintelligence units to provide legal advice, spot legal issues, and provide oversight on

national security matters, including issuance of NSLs. The NSLB has also assigned two NSLB attorneys, one each to the New York and Los Angeles field divisions to provide advice on the use of intelligence techniques, including NSLs, authorized by the Attorney General's NSL Guidelines. Additionally, the FBI OGC said it has added two Senior Executive Service positions within the NSLB to oversee national security matters.

OIG Analysis: The OIG agrees with the FBI's actions to prohibit use of exigent letters. Since our first NSL report, the FBI OGC has sent several communications and reiterated in periodic mandatory NSL training that exigent letters promising legal process in the future are prohibited. The FBI also has clarified the methods by which it may obtain certain non-content telephone and e-mail transactional data in emergency circumstances in accordance with authority in the ECPA, 18 U.S.C. § 2702(c)(4).

The OIG believes that by issuing two ECs, providing mandatory NSL training prohibiting use of exigent letters, requiring NSLB attorneys to regularly attend counterterrorism and counterintelligence operational meetings, placing NSLB attorneys in the New York and Los Angeles field divisions, and adding two Senior Executive Service positions within NSLB, the FBI has taken the steps necessary to provide needed oversight of national security letter matters. While we have no knowledge of additional exigent letters being issued in 2007 subsequent to the March 1, 2007, and June 1, 2007, guidance memoranda, the FBI must continue to emphasize in mandatory NSL training for all personnel assigned to programs overseen by the National Security Branch and to FBI managers the prohibition against using exigent letters and other circumventions of the NSL statutes. In our forthcoming report, we will provide additional recommendations designed to address the findings of our investigation of the FBI's use of exigent letters.

Recommendation No. 8

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

Background: In the course of our first NSL review, we identified a variety of instances in which the FBI used NSLs contrary to statutory limitations, Attorney General Guidelines, or internal guidance or policies. In addition to the use of exigent letters (discussed above in connection with Recommendation No. 7), the instances of improper or illegal use of NSL authorities in 2003 through 2005 generally fell into the following categories:

- issuing NSLs after the investigative authority to conduct the underlying investigation lapsed;

- obtaining telephone toll billing records and e-mail subscriber information concerning the wrong individuals;
- obtaining information that was not requested in the NSL;
- obtaining information beyond the time period referenced in the NSL;
- issuing FCRA NSLs seeking records that the FBI was not authorized to obtain, such as issuing FCRAv NSLs seeking consumer full credit reports for counterintelligence investigations with no international terrorism nexus;
- issuing an ECPA NSL seeking an investigative subject's educational records, including applications for admission, emergency contact information, and associations with campus organizations; and
- issuing NSLs exclusively out of control files rather than from investigative files in violation of FBI policy.

In our first NSL report, we also identified repeated failures to adhere to internal FBI OGC guidance regarding the documentation necessary for approval of NSLs. In our review of 77 investigative files and 293 NSLs in 4 FBI field offices, we found that 60 percent of the investigative files contained one or more of the following infractions:

- NSL approval ECs that were not reviewed and initialed by one or more of the required field supervisors or CDC;
- NSL approval ECs that did not contain all of the required information; and
- NSLs that did not contain the recitals or other information required by the authorizing statutes.

While these infractions did not rise to the level of possible intelligence violations, they were violations of the FBI's internal control policies established to ensure the proper review, use, and tracking of NSLs. For example, review of the NSL package is designed to ensure that errors or inadequate predication are identified and corrected before an NSL is issued. If elements of the approval EC or the NSL are missing, the FBI official signing the NSL cannot be assured that the required predication, specifications of items sought, and statutory authority are correct.

FBI Actions Taken to Address the Recommendation:

New Guidance: The June 2007 Comprehensive Guidance EC provides guidance on the use, requirements, and reporting of NSLs by reminding FBI personnel of the statutory and procedural authorizations and restrictions;

requiring sufficient and independent supervisory and legal reviews; requiring that FBI personnel use "model" NSL and approval EC forms posted on the NSLB's website to ensure all statutory requirements are met and decrease the likelihood of errors; providing checklists for use in drafting the approval EC and NSL, for reviewing responses to NSLs, and prior to disseminating NSL-derived information; and identifying what constitutes a possible intelligence violation and specifying required actions in the event a possible intelligence violation is discovered.

The Comprehensive Guidance EC described the four NSL statutes and the specific types of information that can be obtained from third parties using NSLs. It also emphasized that the content of communications cannot be obtained with an NSL. It clarified that the [redacted] may not be requested through an NSL as a matter of policy, even though these elements have not been determined to be "content" under the ECPA NSL statute.

The guidance cautioned drafters of approval ECs and NSLs to review them carefully to ensure that the information requested by the EC (such as telephone, e-mail, or other account numbers) match those in the NSL and that there are no typographical errors that could result in unauthorized collection and a possible intelligence violation. The guidance also directed that all approval ECs and NSLs must be reviewed for legal sufficiency by the CDC at the field office or by NSLB attorneys at Headquarters before being forwarded to the appropriate designated approving official.

On March 5, 2007, the FBI NSB issued a separate guidance memorandum clarifying the distinctions between the two NSL authorities in the FCRA.

Training: The NSLB has developed a new NSL training module incorporating the findings in the OIG's first NSL report and addressing the common errors discussed in the report such as typographical errors, confusion regarding the two FCRA NSL authorities, and legal review and approval of NSLs. The training refers to the FBI's March 2007 prohibition on the use of exigent letters that promise future legal process and establishes procedures for properly obtaining information in emergency situations in accordance with 18 U.S.C. § 2702. FBI OGC officials told us that the FBI OGC and the NSLB will review the findings of the Inspection Division's review of NSLs in the field and Headquarters divisions to determine if additional procedures or training would improve compliance with this authority.

The FBI OGC has mandated that all NSLB attorneys visiting field offices conduct NSL training during their visits. From March 2007 through

February 2008, 45 of the FBI's 56 field offices and at least 3,042 FBI field and Headquarters personnel involved in preparing and reviewing NSLs received live NSL training from NSLB attorneys.[16] While some Headquarters units had already received NSL training following the release of our first NSL report, mandatory training for personnel in the Counterterrorism, Counterintelligence, and Cyber Divisions was conducted in early May 2007. The NSLB and the Training Division developed an online virtual academy course on NSLs that will be required for all personnel involved in drafting and approving NSLs and will supplement live training. NSL training also has been provided to non-FBI agents serving on the JTTFs nationwide.

On August 21, 2007, the FBI stated in a written response to an OIG request for information, that all FBI employees must complete mandatory training related to NSLs. According to the memorandum, NSL training is offered to new professional staff and to all new Special Agents. A mandatory 2-hour block of instruction is provided during the 17th week of New Agent Training.

Management Meetings, SAC Conferences, and the Annual CDC Conference: As noted above, the FBI Deputy Director told us that NSLs were a major topic of discussion at quarterly Strategy Performance Sessions he chaired via teleconference that were attended by SACs from the FBI's 56 field offices. At the second quarter 2007 sessions, the Deputy Director discussed the findings from the OIG's first NSL report and the steps that the FBI has taken to resolve the OIG recommendations and to implement procedures directed by the Attorney General.

Also, SACs told us that NSL compliance was discussed at the annual SAC conference held in October 2007. NSLB attorneys also provided a presentation on use of NSLs at the CDC conference in July 2007, which included an overview of the findings in the OIG's first NSL report; a discussion of each of the NSL statutes; an overview of the NSLB's guidance on standards and approvals for NSLs; and the required elements of the NSLs, model NSLs, and approval ECs. NSLs also were discussed at squad meetings within field offices, and field office personnel told us that they received numerous e-mails from FBI OGC attorneys and CDCs providing guidance on NSLs.

Office of Integrity and Compliance: As described more fully in Section III of this chapter, the FBI has created a new Office of Integrity and

---

[16] Attendees at these training sessions included Secretaries, Paralegals, Intelligence Analysts, Linguists, Special Agents, Supervisory Special Agents, Section and Unit Chiefs, non-FBI Task Force Officers, Supervisory Resident Agents, Assistant Division Counsels and Chief Division Counsels, Assistant Special Agents in Charge, Special Agents in Charge, FBI OGC attorneys, and Deputy Assistant Directors.

Compliance (OIC) that reports to the Deputy Director. The mission of the OIC is to develop and oversee a program that develops compliance standards and training programs; identifies compliance risks in FBI operations and makes sure that necessary audits are performed; and ensures that national security investigations and other FBI activities are conducted in a manner consistent with laws, regulations, and policies. The OIC is also required to deliver an annual report on compliance issues.[17]

Enhancements to Information Technology: As described in connection with Recommendations Nos. 2 and 4, the new NSL data system is designed to guide the user to more accurately and completely prepare NSLs and route the NSL through the required levels of review. Upon completion of all approvals, the system will generate approval ECs and NSLs for signature by field or Headquarters approving officials. The new NSL data system also is programmed to preclude users from preparing an NSL seeking a consumer full credit report in a counterintelligence investigation that lacks an international terrorism nexus. For each type of NSL, the data system generates a link to the text of the statute to inform the requester what records are authorized to be requested.

Additional Support for the FBI OGC: The FBI OGC has been assigned two new Senior Executive Service positions within the NSLB. One position will head a new section overseeing operational aspects of national security law while the other will head a National Security Law Training and Policy Section. The FBI told us that these positions were filled in February 2008.

FBI OGC officials told us that they are meeting regularly with the NSD and consulting with it on the development of new policy regarding NSLs to address issues identified in our first NSL report. In addition, the NSD and the NSLB conducted 15 national security reviews in 2007, which included a review of the use of NSLs. These reviews were accompanied by NSL training if such training had not recently been given.

OIG Analysis: These initiatives are positive steps that will help the FBI ensure NSLs are issued in accordance with the requirements of national security letter authorities. The Comprehensive Guidance EC compiled in one document NSL guidance and memoranda that had previously been issued piecemeal over several years. This guidance also addressed several of the major findings in our first NSL report, clarified the NSL process, and resolved prior conflicting guidance. We found that the Comprehensive

[17] Deputy Director's Office, Federal Bureau of Investigation, electronic communication to Director's Office, Finance Division, and Inspection Division, Establishment of New FBI HQ Divisions; Director's Office Creation of the Office of Integrity and Compliance, June 5, 2007.

Guidance EC was favorably received by field personnel, who described it during our interviews as "very comprehensive," "very helpful," "a very worthwhile resource," and "thorough and well done."

The FBI has also identified additional opportunities and methods for providing NSL training so all FBI personnel assigned to national security investigations will be aware of the contents of the guidance, including the requirements of the statutes and the required steps in the NSL preparation and approval process.

By issuing the Comprehensive Guidance EC, providing additional training on NSL procedures to field and Headquarters personnel, adding two senior level positions in the FBI OGC to oversee legal issues arising in national security investigations, participating in the NSD's national security reviews, and creating a new NSL data system, we believe that the FBI's ability to comply with NSL authorities will improve significantly.

Recommendation No. 9

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

Background: In our first NSL report, we noted our concern about the ability of NSLB attorneys to obtain accurate and complete information about the FBI's use of NSL authorities. Our review of the FBI's use of exigent letters used by the CAU and "certificate letters" used by the Terrorist Financing Operations Section (TFOS) determined that FBI OGC attorneys were not consulted in advance about tools used by Headquarters CTD units.[18] For example, we determined that NSLB attorneys responsible for providing guidance on the FBI's use of NSL authorities were unaware of the CAU's practice of using exigent letters until late 2004, although CAU personnel had been using these letters as early as 2003.

We also determined that the TFOS issued at least 19 certificate letters to a Federal Reserve Bank seeking financial records concerning 244 named individuals instead of issuing NSLs pursuant to the *Right to Financial*

[18] These certificate letters were used instead of issuing NSLs pursuant to the *Right to Financial Privacy Act* (RFPA). The letters contained certifications that there were "specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power as defined in 50 U.S.C. § 1801."

Privacy Act (RFPA). We also found that the TFOS continued to issue certificate letters despite an August 2004 restriction on this type of request by the FBI Assistant General Counsel. As a matter of policy, the Federal Reserve Bank requires that the FBI issue RFPA NSLs to obtain its records. Accordingly, Federal Reserve attorneys later stated that the Federal Reserve Bank should not have provided the bank records in response to the certificate letters because they were not duly authorized RFPA NSLs.

In our first NSL report, we also found that FBI Headquarters personnel regularly issued NSLs seeking electronic communication transactional records exclusively from "control files" rather than from investigative files, a practice not permitted by FBI policy. This practice prevents a reviewing or approving authority from determining whether the NSLs were issued in the course of authorized investigations or whether the information sought in the NSLs was relevant to those investigations. Documentation of this information is necessary to establish compliance with NSL statutes, the Attorney General's NSI Guidelines, and internal FBI policy.

Accordingly, to ensure that FBI OGC attorneys are consulted about activities undertaken by the NSB, we recommended that the FBI implement measures to promote timely consultation about the NSB's activities, including its operational support activities.

FBI Actions Taken to Address the Recommendation: The FBI OGC mandated in April 2007 that NSLB attorneys involved in national security law matters regularly attend operational meetings to provide legal advice and oversight. Attorneys in the two NSLB units that provide legal advice to counterterrorism operations regularly attend 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 now also regularly attend operational meetings to play a more active legal role. Additionally, 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 has 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.

NSLB attorneys also have provided new NSL training to operational units in the CTD and the Counterintelligence Division. The FBI OGC has posted an NSL training presentation on the NSLB's website and has posted online a virtual academy training course.

The Comprehensive Guidance EC mandates that all NSLs and NSL approval ECs issued by Headquarters components be reviewed and approved by NSLB attorneys. Prior to this mandate, Headquarters officials authorized to sign NSLs were encouraged but not required to consult with the NSLB.

OIG Analysis: The OIG believes that the requirement that all Headquarters-issued NSLs be reviewed by NSLB attorneys, the attendance of NSLB attorneys at meetings of the CTD and the Counterintelligence Division sections to which they are assigned, and mandatory attendance by NSLB attorneys at certain CTD operational meetings should help identify use of new intelligence tools or unconventional requests that may implicate NSL authorities or other intelligence techniques. In addition, mandatory quarterly training of personnel from the specified CTD units should help to ensure that FBI OGC attorneys are consulted about the CTD's activities.

However, we believe the FBI should also have NSLB attorneys similarly participate in operational meetings of other units in the CTD and the Counterintelligence Division in addition to the units that already have been associated with improper use of NSLs. By participating in these operational meetings, it is more likely that the FBI OGC will be in a position to identify and address requests for information that may be inconsistent with the FBI's obligations under the NSL statutes, applicable Attorney General Guidelines, and internal policies governing the use of NSLs.

Recommendation No. 10

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

Background: In our first NSL report, we identified circumstances in which some CDCs and Assistant Division Counsels (ADC) were reluctant to provide an unbiased, independent legal review of NSLs for fear of antagonizing or second-guessing their supervisors, the Special Agents in Charge, who had already approved the underlying investigation. While recognizing that review of NSLs is only one of many issues on which CDCs' independent legal advice is critical, we recommended that the FBI consider measures to ensure that CDCs and ADCs provide thorough and independent oversight of NSL requests.

FBI Actions Taken to Address the Recommendation: The Comprehensive Guidance EC mandates that CDCs and ADCs provide independent legal review of NSLs. The EC stated that the CDCs' and ADCs' legal reviews are separate from and independent of the investigative reviews

conducted by SACs or Headquarters approving authorities. The guidance stated that a legal review should consider whether:

- the information sought in the NSL is relevant to an authorized national security investigation (an investigation to protect against international terrorism or clandestine intelligence activities);
- there is an open and authorized FBI preliminary or full investigation from which the NSL is being issued; and
- there is sufficient predication for the underlying investigation and that predication is sufficiently detailed in the approval EC.

The guidance also stated that if the CDCs, ADCs, or NSLB attorneys determine that legal sufficiency does not exist, they must return the NSL document to the requesting employee for revision. Similarly, if the attorney determines that less intrusive means of obtaining the information are feasible, the NSL will not be approved.

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. The FBI Director stressed at a conference of all SACs the importance of CDCs providing independent legal advice and stressing the role of the head of the office in creating an environment that would foster such advice. The Deputy Director said that at the October 2007 SAC conference and during quarterly Strategy Performance Sessions, he also informed SACs of the need for them to recognize the independence of the CDCs and ADCs. NSL training also emphasizes the requirement that legal review be conducted by CDCs, ADCs, or NSLB attorneys.

The FBI General Counsel and the FBI's senior leadership are still considering how to address the issues identified in our first NSL report arising from the current reporting chain for CDCs. While CDCs continue to report to field division SACs, the General Counsel told us that she is considering whether the CDCs are assigned an unreasonable level of collateral duties that distract them from focusing on their legal duties. If she concludes this is the case, she will discuss the matter with the SACs. As we noted in our first NSL report, this issue involves difficult institutional questions beyond the issue of compliance with NSL authorities.

OIG Analysis: The actions taken by the FBI reinforced that CDCs and ADCs should provide independent legal review of requests to issue NSLs. The Deputy Director of the FBI and the Assistant Director of the CTD both told us that they believe CDCs exercise independent judgment in evaluating NSLs and could not identify any circumstances in which they had not done

so. The Deputy Director stated that it is in the best interest of the SACs to have the CDCs' best, candid advice – even if such advice is not what SACs want to hear. He said he has discussed this issue with SACs during his quarterly meetings with them.

However, further action in response to this recommendation is still being considered by the FBI. We believe it is important for the FBI to resolve the factors weighing for and against modification of the CDCs' reporting chain within the FBI. Review of NSLs is only one of the many oversight functions exercised by CDCs, and the FBI needs the CDCs' independent judgment in ensuring that field agents and supervisors scrupulously observe statutory authorities, Attorney General's Guidelines, and FBI policies governing national security investigations and other authorities.

Recommendation No. 11

Provide guidance and training to Special Agents, Chief Division Counsel, and all FBI officials authorized to sign NSLs on the meaning and application of the Attorney General's Guidelines' proviso calling for use of the "least intrusive collection techniques feasible" to the FBI's use of national security letter authorities.

Background: The Attorney General's NSI Guidelines provide that:

> Choice of Methods. The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of information collection methods that are more or less intrusive, considering such factors as the effect on the privacy of individuals and potential damage to reputation. As Executive Order 12333 § 2.4 provides, "the least intrusive collection techniques feasible" are to be used in such situations. The FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a threat to the national security or the strength of the information indicating its existence. This point is to be particularly observed in investigations relating to terrorism.[19]

We found that the FBI had not provided clear guidance describing how case agents and supervisors should apply the Attorney General Guidelines' requirement to use the "least intrusive techniques feasible"

[19] NSI Guidelines, § I(B)(2).

when deciding how to use and sequence NSLs. While we recognized that there cannot be one model regarding the use of NSLs in all types of national security investigations, and that the FBI cannot issue definitive guidance addressing when and what types of NSLs should be issued at each stage of investigations, we recommended that the FBI provide guidance and training on the use and sequencing of NSLs. In providing such guidance and training, the FBI could highlight and reconcile the important privacy considerations that underlie the Attorney General Guidelines' proviso with the FBI's mission to detect and deter terrorist attacks and espionage threats.

FBI Actions Taken to Address the Recommendation: The Comprehensive Guidance EC requires that as part of their independent legal 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.

On December 20, 2007, the FBI OGC issued guidance to all divisions titled Least Intrusive Techniques in National Security and Criminal Investigations that further addressed this recommendation. The FBI General Counsel told us that a draft of this guidance had previously been provided to civil liberties groups for comment.

OIG Analysis: By providing guidance on application of the Attorney General Guidelines' proviso on the review of NSLs in its Comprehensive Guidance EC, and by issuing the December 20, 2007, guidance on Least Intrusive Techniques in National Security and Criminal Investigations, the FBI has taken significant steps toward addressing this recommendation. However, because the guidance includes many factors to consider when deciding when and how to employ a particular technique, the FBI also needs to provide training on the practical application of this guidance for agents and supervisors.

OIG Conclusions on FBI's Corrective Actions

Based on our analysis of the steps that the FBI has taken, as well as our interviews with FBI leadership, field managers, and personnel involved in the NSL process, we believe that the FBI has made significant progress in addressing the serious problems and deficiencies identified by the OIG in our first NSL report. The FBI's executive leadership, including the Director, Deputy Director, and General Counsel, have expressed their commitment to ensuring that Headquarters and field managers, supervisors, agents, analysts, and support staff understand the seriousness of the FBI's shortcomings in its use of NSLs, the proper use of NSLs, and each of their responsibilities for correcting the deficiencies. The Deputy Director and the

General Counsel continue to emphasize and discuss critical NSL topics at meetings and conferences of executive managers and CDCs.

Since our first NSL report was provided to the FBI, the FBI has issued approximately nine NSL policies and sent numerous other ECs to the field and Headquarters divisions providing guidance on topics that include proper usage of NSLs and statutory and procedural authorizations and restrictions; prohibition on the use of exigent letters; review and redaction of NSL-responsive information; the requirement for sufficient and independent supervisory and legal reviews; and identification of and procedures for submitting possible intelligence violations. The FBI also has developed a new NSL data system with model NSLs and approval ECs that are required to be used when issuing and reviewing NSLs. These measures should eliminate or reduce the types of typographical errors found in the past. To reinforce the new policies and guidelines, FBI OGC attorneys provided NSL training to 45 FBI field offices and at least 3,042 field and Headquarters personnel involved in preparing and reviewing NSLs from March through February 2008. An online virtual academy course on NSLs has also been developed and will be mandatory for all personnel involved in drafting and approving NSLs.

Beyond responding to the OIG's specific recommendations, the FBI has conducted three field reviews on NSL usage to make an independent assessment of the seriousness of the problem and to determine what additional measures were needed. (These reviews are more fully discussed in Chapter Three of this report.)

However, several actions that are necessary to fully satisfy our recommendations are still under development or are in need of additional work by the FBI or the Department. Specifically, the FBI needs to continue to work on:

- providing periodic training to all 56 field offices for those involved in the NSL process. This mandatory training needs to continue indefinitely to address the constant rotation of staff into positions that involve NSL-related work;
- meeting and working with the Chief Privacy and Civil Liberties Officer's NSL Working Group to give additional consideration to label or tag NSL-derived information and to identify when and how often this information is used in analytical intelligence products and provided to law enforcement authorities for use in criminal proceedings;
- fully addressing the current reporting chain for CDCs; and
- providing training on "least intrusive collection techniques" in national security and criminal investigations" to the field.

We believe it is too soon to conclude whether the new guidance, training, and systems put in place by the FBI in response to our first NSL report will fully eliminate the problems with the use of NSLs that we identified and that the FBI confirmed in its own reviews. At the same time, we believe that the FBI has made significant progress in addressing these issues and that the FBI's senior leadership is committed to addressing misuse of NSLs. However, to ensure that adherence to NSL authorities remains permanently embedded in FBI culture and practice, the FBI – and the Department – must be aggressive and vigilant in monitoring compliance with NSL authorities by reinforcing the rules governing the use of NSLs, implementing a sustained process for field and Headquarters verification that NSLs are being handled properly, and ensuring that any violations are identified and reported in a timely manner.

III. Other Corrective Measures Implemented by the FBI and Other Department Components

In this section we describe additional oversight measures implemented in 2007 by the FBI, the NSD, and the Office of the Deputy Attorney General relating to the use of national security letters. We describe the FBI's establishment of a new Office of Integrity and Compliance (OIC) and the NSD's new compliance reviews, termed national security reviews, which review compliance with NSL authorities and other intelligence techniques used by the FBI in national security investigations. In addition, we examine an August 2007 proposal to the Attorney General by the Department's Chief Privacy and Civil Liberties Officer that addresses how the FBI uses and retains NSL-derived information.

A. The FBI's Office of Integrity and Compliance

On July 13, 2007, the FBI announced creation of the OIC.[20] The FBI Director stated that the OIC was established to ensure that national security investigations and other FBI activities are conducted in a manner consistent with appropriate laws, regulations, and policies. According to the FBI's description of the OIC, its mission is "to develop, implement, and oversee a program that ensures there are processes and procedures in place that promote FBI compliance with both the letter and spirit of all applicable laws, regulations, and policies."[21] The OIC is charged with developing

---

[20] Letter from the Attorney General and FBI Director to Richard B. Cheney, President of the Senate, July 13, 2007.

[21] Deputy Director's Office, Federal Bureau of Investigation, electronic communication to Director's Office, Finance Division, and Inspection Division, Establishment of New FBI HQ Divisions; Director's Office Creation of the Office of Integrity and Compliance, June 5, 2007.

compliance standards, training programs, and risk assessments; ensuring that necessary audits are performed; and delivering an annual report on compliance issues.

1. Organization Structure and Operations

Under the organization plan, the Head of the OIC reports to the FBI's Deputy Director. Organizationally, the Integrity and Compliance Program consists of a steering committee (the "FBI Integrity and Compliance Council") that is chaired by the FBI Director and includes as members the Deputy Director; the Associate Deputy Director; the Executive Assistant Director (EAD) of the National Security Branch; the EAD of the Criminal, Cyber, Response, and Services Branch; the EAD of the Science and Technology Branch; the EAD of the Human Resources Branch; the Chief Information Officer; the Head of the OIC; the FBI's Chief Financial Officer; and the General Counsel. The Council is supported by the Executive Management Committees that are responsible for identifying compliance risks in five different functional areas of the FBI's operations: the National Security Branch, criminal investigations, investigative support, administration, and information technology.

Each Executive Management Committee is chaired by the EAD responsible for the functional area and includes as members the Assistant Director from the functional area; a Deputy General Counsel from the FBI OGC; representatives from the OIC; and other members as the chair finds necessary. The Executive Management Committees are required to meet at least four times a year to analyze the nature of the compliance risks facing their functional areas; identify specific risk areas; and assess and establish policies, procedures, and training to mitigate those risks. Within 2 days of an Executive Management Committee meeting, the committee chair is required to assess and rank the compliance risks, designate a "risk owner," and document the results with the OIC. The risk owner is responsible for further assessing the risk, determining whether corrective actions are warranted, and developing mitigation plans.

To conduct the risk assessments, the most significant risks identified by the Executive Management Committees are to be subjected to a detailed analysis by a compliance risk assessment team (called a Red Team) created by the risk owner with the assistance of the OIC. The Red Teams are staffed with a representative from the OIC, two subject matter experts from the organization having primary responsibility for the risk area, and a representative from the FBI OGC. The Red Teams will review the law, FBI policies, training, and monitoring requirements related to the issue. The Red Teams were directed to produce within 60 days of receiving the tasking a report analyzing the risks and developing a risk mitigation plan. Those reports will be provided to the risk owner and the pertinent Executive

Management Committee chair for review and implementation of measures to mitigate the risks. In addition to reports of individual risks, the FBI planned to require the OIC to prepare a consolidated annual report on compliance risks throughout the FBI. In February 2008, the FBI informed us that it had decided to eliminate the requirements that Red Teams develop risk mitigation plans (but did not eliminate the risk assessment report) and that the Executive Management Committees prepare a consolidated annual report on compliance risks throughout the FBI. In addition, the FBI stated that the Executive Management Committees are to provide an annual report on "the state of the Integrity and Compliance program." Although it is not clear that the revised annual report will include a consolidated assessment of compliance risks, we believe that such a consolidated assessment listing all identified risks will be valuable to the FBI and the Attorney General.

FBI officials told the OIG that they also plan to divide personnel assigned to the OIC into two units: the Compliance Operations Unit and the Compliance Policy and Analysis Unit. According to the FBI, the Compliance Operations Unit will support implementation of compliance policy and standards within FBI divisions, including analyzing operations and legal requirements; identifying specific compliance risk areas; prioritizing the risks; and establishing policies, procedures, and training to ensure compliance. The OIC's Compliance Policy and Analysis Unit will establish compliance policy, including a methodology for assessing risk (described below), compliance standards, and monitoring and auditing procedures. The Compliance Policy and Analysis Unit also will develop and provide training and monitor the overall compliance program.

The OIC is designed to be independent from, but expected to work closely with, the FBI's Inspection Division to identify high-risk areas. The Head of the OIC said that the Inspection Division would include monitoring of identified compliance risks (which will be incorporated into the Inspection Division's inspection protocols) in its inspections of Headquarters and field divisions. According to OIC documents, the Inspection Division is expected to provide the OIC with inspection data gathered during its inspections to support the OIC's compliance monitoring and will conduct audits as needed to support the compliance oversight program.

As of January 2008, the Attorney General and the Office of Management and Budget had approved the establishment of the OIC. Congressional committees were notified on November 21, 2007. According to the Head of the OIC, the FBI's Corporate Resource Planning Board (which approves the establishment of positions) and the FBI's Position Review Board (which determines whether positions are staffed with Special Agents or support staff) authorized 12 positions for the OIC, including a Senior

Executive Service position, 1 Secretary, 1 Special Agent (on a detail/rotation), 5 Attorneys, and 4 Management and Program Analysts.[22] In addition, two attorneys from the FBI's Office of General Counsel were later transferred to the OIC, along with the ethics/standards of conduct function that they support. As of February 2008, the OIC had 12 personnel on board. The FBI told us that the OIC will re-evaluate its staffing and organizational structure as the program continues to mature. As of January 2008, each of the five Executive Management Committees had met three times, and Red Teams were conducting reviews to analyze the top compliance risks in each of the five functional areas.

2. Risk Assessment Process

The procedures describing the OIC's operations were still in development during the OIG's review. However, the Head of the OIC provided information to the OIG on the assessment tool that the Executive Management Committees intended to use to assess and rank identified risks. The assessment tool allows the Executive Management Committees to assign a numerical value to internal and external factors associated with each risk, including such considerations as the complexity of the program or activity, environmental factors (such as whether the program is a new activity or involves new technology), workforce factors (such as whether training related to the activity is available), and potential privacy and civil liberty impacts. The tool also includes "weighting" factors, such as the frequency and potential magnitude of any potential harm associated with the risk.[23] Using the numerical values assigned to all the factors, the assessment tool calculates an overall score that enables the Executive Management Committees to rank the risks. The chair of each committee provides independent judgment regarding the recommended rankings and approves the ordering of the potential risks. The committee Chairs are to provide the FBI Deputy Director and the OIC with their committee's assessment of the five highest-ranked risks. The FBI Director, as chair of the FBI Integrity and Compliance Council, is responsible for determining whether the risk identification and rankings are "sound."

After the most important risks have been identified, Red Teams will use an OIC-developed draft compliance checklist to guide their reviews. In

---

[22] Initially, the OIC was authorized to have two Special Agent positions, but one of the positions was subsequently converted to a support position.

[23] NSLs will not be subjected to the risk assessment process. The Head of the OIC told the OIG that the OIC risk identification process will not be used to assess risks associated with NSLs because the reviews conducted by the OIG in 2006 and 2007 and by the FBI Inspection Division in 2007 already identified those risks and corrective actions (including updating policy and guidance and providing training) are being taken in response to those reviews.

addition, the OIC developed a compliance risk assessment report format for compiling the Red Teams' findings that addresses specific elements related to the risk. The risk assessment report format includes:

- a summary of the risk;
- a review of the legal authorities relevant to the operations being reviewed;
- an assessment of the internal policies, procedures, and cost controls in place;
- an assessment of the training provided related to the at-risk activity;
- a listing and assessment of the existing data that management has available to identify or assess potential compliance failures related to the risk;
- a discussion of potential compliance failures that already have been identified; and
- a brief assessment of potential corrective actions identified by the Red Team to ameliorate the risk under review.

As noted above, the Red Teams' reports should be provided to the risk owner and the responsible Executive Management Committee within 60 days after the initial Red Team meeting. The risk owner is then expected to develop and implement a mitigation plan for ameliorating the compliance risks.

3. OIG Analysis

While the OIC is in the developmental stages and its procedures and expected outcomes are not yet fully defined, we believe it can be a valuable tool for the FBI. As planned, the OIC can provide the FBI with a structured process for identifying compliance requirements and risks, assessing existing control mechanisms, and developing and implementing better controls to ensure compliance with law, regulations, and policies. Senior FBI management, including the FBI Director, told us that they are committed to supporting the successful implementation of the compliance program.

However, we believe that the OIC faces significant challenges in fulfilling its mission. One challenge for an internal compliance program – particularly one staffed with technical experts from the program or office under review – is to identify unknown or emerging risks. Consequently, such a compliance program may unduly focus on risks that are already known and are already being addressed. However, the Head of the OIC told

the OIG that the FBI is attempting to meet this challenge by involving individuals at all levels of the program or office in the risk identification process. Additionally, the FBI stated that the OIC staff, through internal and external contacts and reviews, provides advice to the Executive Management Committees on information it develops concerning possible compliance concerns.

We also note that a compliance oversight process in which the subject program or office that "owns" a set of identified compliance risks also rates the severity of the risks may introduce a tendency or bias toward focusing on risks or activities most important to the risk owner. These activities may be different from those risk-sensitive activities viewed as most significant by an independent entity conducting a compliance review. While the OIG recognizes that the Executive Management Committees that identify and prioritize risks include members from the FBI OGC and FBI executive management who are expected to provide objective compliance expertise (as opposed to operational or technical expertise), the final determination of how risks are ranked lies with the "risk owning" office. According to the FBI, having the owning office rank the risks will provide "buy in" on the need to address the risk. However, we believe that objective ranking of risks for further assessment and remediation is a critical component of a successful compliance program. Consequently, although the rankings are reviewed by the Director and Deputy Director, we believe that the FBI must be vigilant to ensure that the ranking of risks by the risk owners is objective.

In addition, we note that the OIC currently has an authorized permanent staffing level of only 14 positions and will depend on FBI personnel in other offices to carry out many functions critical to the success of the new compliance program.[24] As presently envisioned, the OIC appears to serve as a coordinator rather than an entity with sufficient independent resources and a capability to identify and assess compliance risks. For example, as described above, the Red Teams responsible for conducting the detailed risk assessments are composed primarily of personnel from the risk-owning office and the FBI OGC, while the OIC's role is to facilitate the assessment process and receive the results for the Executive Management Committees. According to the FBI, this structure is modeled on corporate practices. Similarly, to conduct compliance monitoring, the OIC will rely on Inspection Division personnel to conduct the monitoring or inspections. However, we believe this can place FBI agents in a difficult position when they are only temporarily assigned the responsibility to inspect and potentially criticize the actions of FBI colleagues and units since after their

[24] The number of permanently assigned OIC staff is much lower than the number of employees in the Inspection Division, which currently is assigned 30 employees.

rotation in the Inspection Division, they often return to work alongside the FBI employees and supervisors whose actions they reviewed during their rotation. Accordingly, to make the difficult judgment calls regarding weaknesses and compliance problems that will arise in the course of the OIC's work, we believe that the FBI should consider providing the OIC with a substantial permanent staffing level so that it can develop the skills, knowledge, and independence to lead or directly carry out the critical elements of a new compliance program.

B. National Security Division

In September 2006 the Department established the National Security Division (NSD) to consolidate the supervision of the Department's primary national security elements within a single division. The NSD was created by combining the Office of Intelligence Policy and Review (OIPR) and the Counterterrorism and Counterespionage Sections that were formerly part of the Criminal Division. In July 2007 the Department announced that it would reorganize the NSD and, as a part of the reorganization, would create within the NSD an Office of Intelligence to replace the OIPR. The mission of the Office of Intelligence is "to ensure that national security investigations are conducted in a manner consistent with the nation's laws, regulations, and policies, including those designed to protect the privacy interests and civil liberties of [U.S.] citizens."[25] On September 24, 2007, the Assistant Attorney General for the NSD issued a memorandum that detailed the structure and operations of the three sections that comprise the new Office of Intelligence.[26] However, in February 2008, the NSD informed the OIG that the reorganizations announced in September 2007 had not been completed, as the Office of Intelligence had not yet been created. We describe below the operations of the Office of Intelligence and the roles of each of the three sections as they were announced in September 2007.

1. Office of Intelligence

The Office of Intelligence will consist of three sections: the Oversight Section, the Operations Section, and the Litigation Section (see Chart 2.1). The Oversight Section will oversee all aspects of the FBI's national security program and its use of intelligence techniques to support that program, including NSLs. The Operations Section will conduct intelligence operations work, such as representing the government in presenting applications to the Foreign Intelligence Surveillance Court. The Litigation Section will

---

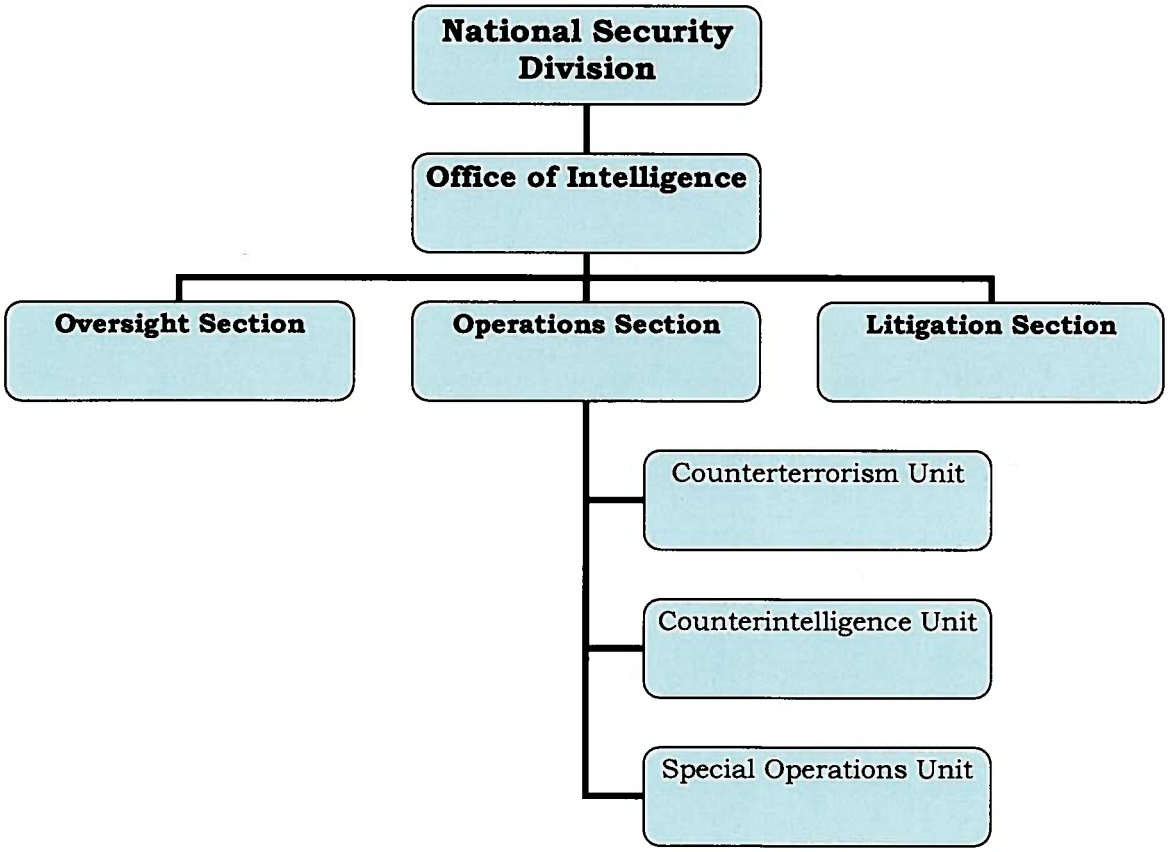
[25] Letter from the Attorney General and FBI Director to Richard B. Cheney, President of the Senate, July 13, 2007, 1.

[26] Assistant Attorney General, National Security Division, memorandum to all National Security Division Employees, September 24, 2007.

supervise and coordinate criminal and civil litigation matters related to the FISA and other intelligence issues.

Attorney staffing levels for the Office of Intelligence will remain the same as its predecessor offices – approximately 85 attorneys – and it was anticipated that the attorneys would rotate among various units and sections within the Office of Intelligence. The majority of the attorneys are to be assigned to the Operations Section and may serve on rotating assignments among the three units that comprise that section (the Counterterrorism Unit, the Counterintelligence Unit, and the Special Operations unit). In addition, some attorney positions in the Oversight and Litigation Sections will be filled by attorneys from the Operations Section on a rotating basis. Attorneys also will be expected to provide support to other sections where appropriate. For example, Operations Section attorneys that prepare FISA applications would be expected to provide support to the Litigation Section if the FISA applications are at issue in related criminal trials.

CHART 2.1
Organization of the Office of Intelligence



Source: Department of Justice, National Security Division

2. Oversight Section

According to NSD officials, the mission of the Oversight Section will include functions previously exercised by OIPR as well as several new oversight functions that represent a significant expansion of the Department's oversight of the FBI's investigative operations. OIPR's oversight was focused primarily on the FBI's use of FISA authorities and included "accuracy reviews" to ensure the accuracy of FBI declarations to the Foreign Intelligence Surveillance Court and "minimization reviews" to ensure that FISA information was handled appropriately. These minimization reviews are conducted to assess the FBI's compliance with the FISA requirement that the FBI implement procedures "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons. . . ."[27] OIPR also previously conducted reviews of FBI notices related to national security investigations to ensure compliance with the Attorney General Guidelines.

In April 2007 OIPR expanded its oversight functions to include most aspects of the FBI's national security program and its use of national security tools, including national security letters.[28] These oversight functions were implemented under OIPR; the NSD did not wait for the establishment of the Oversight Section. According to the NSD's September 24, 2007, reorganization memorandum, the Oversight Section will take over the responsibility of reviewing national security investigation case files in FBI field offices and Headquarters divisions to provide guidance on a wide range of issues, including compliance with Attorney General Guidelines, the use of NSLs, and the predication for national security investigations. In 2007, OIPR began reviewing all FBI referrals to the IOB and will report to the Attorney General any recurring problems or trends. In addition, as a part of the NSD's overall mission, Office of Intelligence

---

[27] 50 U.S.C. §§ 1801(h)(1) and 1821(4)(A). During the minimization audits, attorneys from OIPR visited FBI field offices to assess the FBI's minimization of the results of FISA-approved electronic surveillance and physical searches; counsel case agents, intelligence analysts, and linguists on specific issues; and provide training to those involved in the minimization process.

[28] According to an NSD Associate Counsel, because intelligence investigations typically focus more on identifying and addressing threats than on prosecuting criminals, Department attorneys previously had been less involved in the FBI's national security investigations than they had been in traditional criminal investigations. In traditional criminal investigations, Department attorneys approve some investigative steps, obtain search warrants, and guide the conduct of the investigation in preparation for prosecution. In contrast, the primary involvement of Department attorneys in national security investigations resulted from their role as representatives to the Foreign Intelligence Surveillance Court.

attorneys will provide training on legal and regulatory compliance issues. Each of these oversight activities, which OIPR began conducting in 2007, is discussed further in the following sections.

a. National Security Reviews

In response to the OIG's March 2007 report on NSLs, the NSD instituted what it terms national security reviews to examine whether the FBI is using a variety of intelligence techniques, including NSLs, in accordance with applicable laws, guidelines, and policies.

From the time the review process was established in April 2007 through December 30, 2007, the NSD completed national security reviews at 14 FBI field offices and 1 Headquarters division. The national security reviews focused on the initiation and maintenance of national security investigations to verify compliance with laws, guidelines and policies, as well as the FBI's use of NSLs. According to NSD personnel, the scope of the reviews will expand over time to encompass other elements of the national security investigative program, such as undercover operations, and how information related to national security investigations has been disseminated outside of the FBI.

The NSD worked with the FBI to select the 15 offices to be reviewed in 2007. The FBI OGC selected as the first field office to be reviewed one that had received a particularly favorable review in its last inspection by the FBI's Inspection Division. The NSD selected the remaining 13 field offices and 1 Headquarters division with the FBI OGC's concurrence based on several considerations. To gain experience before reviewing a large field office, the NSD scheduled the reviews so that the first reviews were of small and medium-sized FBI field offices. Two larger field offices were scheduled for review in the last quarter of 2007. For 2008, the NSD plans to conduct reviews at 14 additional FBI field offices and 1 Headquarters' division. In 2008, the NSD plans to select for national security reviews offices that have higher numbers of national security investigations about which the NSD has had questions (identified in its review of FBI initiation notices of national security investigations) and also to continue to conduct FISA minimization and accuracy reviews.[29]

The national security reviews are conducted by teams consisting of NSD attorneys with intelligence experience and representatives from the FBI OGC. Personnel from the Office of the Chief Privacy and Civil Liberties Officer may also attend reviews but they are not considered part of the

---

[29] The FBI is required to provide the NSD with approval memoranda signifying the initiation of national security investigations.

review team. The teams conducting the national security reviews typically consist of six members: three NSD attorneys, two FBI OGC attorneys, and one FBI Special Agent.

During each of the 15 reviews completed as of December 31, 2007, the team members worked in pairs to review approximately 25 selected case files. The case files were selected to include: (1) case files that had already been identified as being of interest based on OIPR's review of national security investigation notices; (2) case files generated in both counterintelligence and counterterrorism investigations; and (3) case files that included NSLs. For most case files, the team reviewed each NSL issued since January 1, 2006, but selected only a sample from case files that contained a large number of NSLs.

To guide the reviews, attorneys in OIPR developed a checklist that identified the information to be collected from each case file. The checklist was modeled on the data collection instrument used by the OIG for our first NSL report. It contained additional data points to capture information on the initiation and maintenance of national security investigations and on the use of other intelligence techniques and procedures.

According to an NSD Associate Counsel, prior to on-site visits OIPR attorneys provided training to team members on how to conduct the reviews and record their results. On October 8, 2007, the NSD issued a memorandum setting forth details of its process for conducting future national security reviews and for communicating results to the NSD's senior leadership.

At the conclusion of each national security review, the team prepared a narrative report of its findings. A summary of these reports follows.

The NSD provided the OIG with reports of its reviews of national security investigations in 13 FBI field and Headquarters offices that it conducted from April 2007 through November 2007.[30] The reviews focused on three areas: examinations of the initiations, extensions, and conversions of national security investigations; evaluations of all aspects of the use of NSLs issued between January 1, 2006, and the date of NSD's review; and determinations as to whether possible IOB violations had been reported to the FBI OGC. The NSD generated separate reports for each review that included overall observations, along with specific findings regarding each investigation and NSL it reviewed.

---

[30] The OIG reviewed the first report that was finalized, along with 12 draft reports. After completion of our analysis, the NSD told us that it has finalized all 13 reports.

During its reviews, which ranged from 2 to 5 days in length, the NSD reviewed a total of 1,047 NSLs in 276 investigations. The NSD reviewed as few as 4 NSLs in 2 investigations in 1 office and as many as 130 NSLs in 23 investigations in another office. The reviewed investigations included 150 counterterrorism matters and 126 counterintelligence matters. We were not able to determine from the NSD reports the statute under which all the NSLs that it reviewed were issued. However, approximately 80 percent of the NSLs for which we were able to identify the statute were issued under ECPA.

The NSD's findings were consistent with those identified in our first NSL report on the FBI's use of national security letters. The NSD reviews examined overcollections, errors in approval ECs and NSLs, inconsistencies between approval ECs and NSLs, the inability to locate responsive records, failure to include the U.S. person status of the subject of the investigation or the target of the NSL, and failure to describe in the approval EC the relevance of the records sought to the investigation. The NSD found that:

- The FBI obtained information it did not request or that it was not entitled to receive. The NSD observed that a mismatch between the FBI's requested date range and the manner in which third parties maintained their records often caused the overcollections. Additionally, there was little documentation of overcollections or documentation of the disposition of these matters.
- Errors occurred in the NSLs and approval ECs because case agents relied on previously drafted documents that were outdated or no longer valid.
- There were "disconnects" between the NSL and approval ECs, including approval ECs that did not specifically state the information being requested or that differed from the records requested in the NSLs.
- The information provided by third parties to the FBI was not always retained in the investigative case files because the original documents were provided to analysts or FBI Headquarters.
- The approval ECs did not consistently reference the U.S. person status of individuals, which is required for purposes of congressional reporting.
- The relevance of information requested in the NSLs to the underlying investigations was not consistently explained in approval ECs.

In addition to these issues, the NSD reviews identified other noteworthy matters. In our first NSL report, we noted that a field office reported to the FBI OGC that it had obtained information from an asset and had not issued an NSL to obtain that information. The FBI OGC did not report the matter to the IOB – a decision that we disagreed with and the FBI later changed. In its reviews, the NSD found instances in two field offices in which assets provided financial records to the FBI, but the FBI did not issue NSLs to obtain the records, as required by the *Right to Financial Privacy Act* NSL statute. Neither of these matters had been reported to the FBI OGC prior to the NSD review. The NSD also found instances in which the current Patriot Reauthorization Act non-disclosure and confidentiality models were not being used, the required certifications were missing, or there was no stated basis in the approval ECs for imposing these obligations. In addition, the NSD identified instances in which NSLs were served during lapses in investigations, contrary to the NSL statutes and the Attorney General Guidelines; consumer full credit reports obtained in response to *Fair Credit Report Act* NSLs seeking limited credit information were not successfully redacted and the reports were fully readable; and a field office uploaded into the ACS system unauthorized information obtained in response to NSLs.

The NSD made several recommendations to address issues that it determined warranted further examination. To address unauthorized collections, the NSD recommended that the FBI develop guidance that more specifically provides instruction on:

- overcollected information;
- sequestration of information with the CDCs;
- destruction or other disposition of improperly obtained information;
- uploading of information into FBI databases; and
- verification of removal (of overcollected information) from FBI electronic files and databases.

To prevent the receipt of unauthorized information, the NSD also recommended that the FBI work more closely with NSL recipients by revising the standard language used in NSLs in describing the time periods for which records are requested.[31]

---

[31] This NSD recommendation may have already been addressed when, in May 2006, the FBI OGC revised the model attachment for ECPA toll record NSLs. The NSD reviewed NSLs issued on or after January 1, 2006. Since we are unable to determine the dates of the NSLs that the NSD reviewed, we are unable to determine whether the

(Cont'd.)

To address errors and inconsistencies between the NSLs and approval ECs, as well as missing required language, certifications, or an established nexus between the investigation and the records requested, the NSD recommended that:

- standardized NSL forms from the FBI OGC website be used;
- case agents be provided instruction and training to ensure that the information requested in the NSLs matches what is requested in the approval ECs; and
- case agents be provided instruction and training on the importance of describing in NSL approval ECs a sufficient nexus or relevance between the investigation and the information requested.

To address the FBI's inability to locate records received in response to NSLs, the NSD recommended that:

- case agents keep original results in the investigative case files and provide copies to analysts and FBI headquarters; and
- the FBI OGC initiate a tracking system so case agents can determine whether NSLs have been served and whether the NSL recipients have provided responses to the FBI.

The NSD also recommended that the Department establish a working group of representatives from the NSD, the FBI, and the Office of the Deputy Attorney General to review the results of the NSD's national security reviews. The NSD suggested that the NSL Working Group recommend changes to guidelines, practices, and training to establish clear, concise, well-documented, and consistent procedures for implementing the NSL statutes and Attorney General Guidelines.

b. Reviews of FBI Reports to the IOB

As directed by the Attorney General in March 2007, the NSD also is responsible for reviewing all FBI reports of possible intelligence violations to the IOB in order to identify recurring problems and assess the FBI's response to such violations. According to NSD officials, the review process focuses on whether these reports indicate that a change in policy, training, or oversight mechanisms is warranted. The Oversight Section also will report to the Attorney General twice a year and inform the Department's

---

unauthorized collections occurred prior to or after the issuance of the new model attachment.

Chief Privacy and Civil Liberties Officer of any referrals that raise "serious civil liberties or privacy issues."

As of November 30, 2007, the NSD had forwarded its initial semiannual report to the Attorney General. The report provided a statistical summary and description of reports to the IOB from January 1, 2007, through June 30, 2007, and reported the NSD's observations regarding trends and patterns in the notices of reports to the IOB. Chief among these were observations relating to the reporting of national security investigations by FBI field offices, compliance with Foreign Intelligence Surveillance Court orders, and maintaining current investigative authority for ongoing operations. The NSD report recommended that existing policy regarding reporting by the FBI to the NSD of the initiation of national security investigations needed to be modified. In addition, the NSD recommended additional guidance and training to avoid lapses in investigative authority and to clarify the scope of records that may be obtained through ECPA NSLs.

c. Training and Outreach

In addition to conducting national security reviews, the NSD plans to provide training on legal and regulatory compliance issues for its attorneys and for FBI agents and analysts and to conduct outreach to other members of the Intelligence Community.

3. OIG Analysis

Based on our review of documents describing the NSD's national security reviews, our interviews of NSD officials, the data collection instrument, and the report of the results of the first national security review, we believe the national security reviews are important additions to other audits and oversight measures implemented by the FBI (described in this chapter and in Chapter Three of this report). In particular, we believe the experience of NSD attorneys and other personnel in the new Office of Intelligence will bring important expertise to the oversight of NSLs and other intelligence techniques.

We also believe that the scope of the NSD's reviews is reasonable. These reviews examine compliance with laws, guidelines, and policies relating to the FBI's use of various intelligence techniques, including NSLs. Further, the NSD's plan to shift the focus of its reviews over time to encompass other aspects of the FBI's national security investigations seems reasonable and appropriate.

However, it is important that sufficient resources be allocated, both in the FBI and NSD, to keep pace with the plans to complete approximately 15 national security reviews per year. Moreover, as the results of the FBI's

three 2007 NSL reviews (discussed in Chapter Three of this report) are fully evaluated, the NSD should re-evaluate whether adjustments to the scope and focus of the national security reviews are warranted.

C. National Security Letter Working Group

In response to a directive in the Patriot Reauthorization Act and our first NSL report, the Attorney General directed the Department's Privacy Officer, working with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (DNI), to convene a working group (NSL Working Group) to examine how NSL-derived information is used and retained by the FBI.[32] In addition to the Privacy Officer and the DNI's Civil Liberties Protection Officer, the NSL Working Group included the senior privacy official of the FBI and representatives from the Department's Office of Legal Policy, NSD, and the Office of the DNI Director.

In our first NSL report, the OIG noted the proviso in the Attorney General's NSI Guidelines that national security investigations should use the "least intrusive collection techniques feasible" to carry out the investigations.[33] The OIG reported that we found no clear guidance on how Special Agents should reconcile the Attorney General Guidelines' limitations with the expansive authority provided in the NSL statutes. Our concerns over the lack of formal guidance were magnified because of the volume of NSLs generated by the FBI each year and because the information collected is retained for long periods in databases available to many authorized law enforcement personnel. To better identify NSL-derived data retained by the FBI, we recommended, among other things, that the FBI consider measures to label or tag NSL-derived information in its databases.

In August 2007 the NSL Working Group completed a proposal for minimization and retention of certain NSL-derived information and sent the proposal to the Attorney General for approval.[34] The proposed policy and

---

[32] Section 119(f) of the Patriot Reauthorization Act, states:

Minimization Procedures Feasibility – Not later than February 1, 2007, or upon completion of review of the report submitted under subsection (c)(1), whichever is earlier, the Attorney General and the Director of National Intelligence shall jointly submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report on the feasibility of applying minimization procedures in the context of national security letters to ensure the protection of the constitutional rights of United States persons.

[33] NSI Guidelines, § I(B)(2).

[34] The NSL Working Group adopted the definition of "minimization procedures" as it is used in FISA 50 U.S.C. § 1801(h):

(Cont'd.)

recommendations relate to data obtained by the FBI in response to NSLs seeking financial and consumer credit information as well as data obtained in response to NSLs seeking telephone billing records, telephone and e-mail subscriber information, and electronic communication transactional records.[35] However, the recommendations of the NSL Working Group were not acted upon by the Attorney General. In February 2008, the Privacy Officer told the OIG that the proposal had been withdrawn from the Office of the Attorney General and that the Privacy Officer intended to reconvene the Working Group. According to the Privacy Officer, the Working Group needs to make specific enhancements to both the proposal and related procedures to describe more fully the research, clarify the Working Group's findings, and potentially strengthen its recommendations. Below, we describe the findings, reasoning, and recommendations contained in the proposal submitted to the Attorney General by the NSL Working Group, followed by our analysis and recommendations. We offer these comments for the NSL Working Group to consider as it prepares to re-examine these important issues.

1. Evaluation of Existing Controls and Guidelines

The NSL Working Group initially examined existing controls and guidelines that protect privacy interests regarding the acquisition and use of NSL-derived information. The report of the NSL Working Group noted that NSLs can only be used in connection with national security investigations, must be approved by a senior FBI official, and provide access only to limited information. Further, the report noted that NSL-derived information is subject to standard agency records retention rules, must be disseminated and retained only in accordance with applicable Attorney General Guidelines, and can only be accessed through FBI databases by authorized

---

> (1) specific procedures . . . that are reasonably designed in light of the purpose and technique of [NSLs] to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that non-publicly available information, which is not foreign intelligence information . . . shall not be disseminated in a manner which identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance.

Chief Privacy and Civil Liberties Officer, U.S. Department of Justice, memorandum to the Attorney General, U.S. Department of Justice, August 17, 2007, 6. (NSL Working Group Memorandum).

[35] The report stated that the Department planned to use the findings of the NSL Working Group in preparing the report to Congress required by § 119(f) of the Patriot Reauthorization Act on the "feasibility of applying minimization procedures in the context of national security letters to ensure the protection of the constitutional rights of United States persons." NSL Working Group Memorandum, 1.

individuals for official purposes. Based on this evaluation, the NSL Working Group concluded that "significant limitations already exist governing the proper use of NSLs."[36]

The NSL Working Group's report concluded that the FBI has made "significant progress in identifying and rectifying concerns about the FBI's compliance" with NSL authorities.[37] For example, the NSL Working Group cited the FBI OGC's June 1, 2007, Comprehensive Guidance EC that directs Special Agents to review information received in response to NSL requests; improvements to the FBI's electronic data systems; the establishment of the FBI OIC; and the new oversight activities of the NSD.

The NSL Working Group report concluded that controls provided by existing statutes and guidelines, if properly followed, effectively minimize the collection of information on U.S. persons and protect privacy interests. However, the NSL Working Group also stated that further enhancements to privacy safeguards, which we discuss in the next section, would be appropriate.

2. Additional Privacy Enhancements Recommended by the NSL Working Group

To improve privacy safeguards for information acquired with NSLs, the NSL Working Group proposed initial minimization procedures applicable to information derived from RFPA, FCRA, and ECPA NSLs. Some of the proposed procedures amplify recently implemented requirements imposed by the FBI in response to the OIG's first NSL report. The NSL Working Group stated that its recommendations recognized that "information that appears to be of little value today" may later become significant. It also stated that private business practices calling for routine destruction of older records helped guide the group's recommendations.[38]

a. Financial and Credit Information

According to the NSL Working Group's recommendation, NSL-derived financial and credit information should initially be reviewed by the case agent or analyst to determine whether the information has "investigative value." The NSL Working Group defined information as having "investigative value" if the information "contributes to a national security investigation or to an authorized intelligence collection requirement."[39] The

---

[36] Id. at 5.

[37] Id. at 6.

[38] Id. at 6-7.

[39] NSL Working Group Memorandum, Attachment, 1.

determination of whether information has investigative value is to be made by "the case agent or other employee familiar with the scope of the investigation and its objectives."[40]

The NSL Working Group noted that information requested in an NSL may be produced in paper or electronic form and therefore established slightly different procedures for making the "investigative value" determination given the different formats. The NSL Working Group stated that financial or credit information received in electronic form should be uploaded onto a desktop computer and reviewed to identify non-responsive data and to determine if it has investigative value. Under the proposal, data from responsive financial or credit paper documents may also be temporarily entered into a desktop computer – but not into an FBI-wide database – so that it may be more easily reviewed to determine if it has investigative value.

Under the NSL Working Group's proposal, FBI personnel may upload into FBI databases and include in analytical products only financial and credit information that is determined to have "current or reasonably potential" investigative value. The electronic media and paper copies of all responsive documents, whether determined to have investigative value or not, are to be retained in designated sections of the investigative file.

b. Electronic Communication Transactional Data

Under the proposal, information derived from ECPA NSLs (telephone toll billing records, telephone and e-mail subscriber information, and electronic communication transactional records) need only be determined to be responsive to the NSL in order to be uploaded into any appropriate FBI-wide database (such as the ACS system or Telephone Applications database). Unlike the limitations imposed on NSL-derived financial and credit information (requiring an initial determination that the information has "investigative value"), the NSL Working Group's proposal would not restrict the initial uploading of these records into FBI databases. The NSL Working Group concluded that electronic communication transactional information cannot be evaluated in isolation, but must be uploaded so that link analysis and other analytical measures can be used to determine its investigative value. The NSL Working Group also stated that it based its recommendation on reduced privacy interests associated with ECPA NSL records. As with financial and credit data, the NSL Working Group's proposal requires retention of the electronic media containing the data in designated sections of the investigative file.

---

[40] Id.

3. Other Enhancements Considered but Not Recommended

According to its report, the NSL Working Group also considered but decided not to recommend additional minimization procedures. The NSL Working Group also recommended against applying any time limitation on the retention of NSL-derived information beyond the existing routine agency data retention protocols relating to investigative files. Instead, the NSL Working Group stated that information found to have investigative value should remain available for unrestricted access by authorized users of the ACS system or the Investigative Data Warehouse until it is archived in accordance with applicable National Archives and Records Administration disposition schedules.[41]

In addition, the NSL Working Group recommended against "tagging" NSL-derived information so that it would be identifiable as such if it is used in analytical intelligence products or transferred to other Intelligence Community-wide computer systems, concluding this would cause "an undue burden on the operation of such an important tool." Further, the NSL Working Group stated that planned enhancements to the FBI's information technology systems will allow NSL-derived information to be segregated in the FBI OGC's NSL tracking database. Consequently, the NSL Working Group concluded that "tagging" NSL-derived data would not provide "any measurable value for privacy protections . . . ."

The NSL Working Group decided against recommending that the FBI delete NSL-derived data from its data systems when cases are closed. According to the NSL Working Group's report, requiring the deletion of NSL-derived data upon case closing would have potential negative impacts on the investigative process because closing a case is not necessarily indicative of a subject's innocence. For example, the FBI sometimes closes counterintelligence cases when the subject leaves the country, but may re-open the case if the subject returns. Further, the NSL Working Group stated that information gathered during an investigation that is closed could have investigative value in other cases.

---

[41] The length of time that the FBI retains investigative information, whether in paper or electronic format, depends on several factors, including the case type (for example, intelligence or criminal investigations) and other characteristics of the case (for example, if it involved a "most wanted" suspect). In general, information related to intelligence investigations is retained in the FBI's files (either in the paper case file or in the FBI's electronic systems) for 30 years after a case is closed, and information related to criminal investigations is retained for 20 years after a case is closed. After that time, the case information is reviewed, and information that is identified for permanent retention is transferred to the National Archives and Records Administration (NARA) for storage. Any cases not meeting the criteria for permanent retention and transfer to the NARA are destroyed.

4. OIG Analysis of the NSL Working Group's Report and Recommendations

The OIG believes that the NSL Working Group should consider further whether and how to provide additional privacy safeguards and measures for minimizing the retention of NSL-derived information.

First, the NSL Working Group's conclusion that "significant limitations already exist governing the proper use of NSLs" could easily have been written in March 2006 when the Patriot Reauthorization Act directed the OIG to review the FBI's use of NSLs. At that time, the NSL statutes, Attorney General Guidelines, and internal FBI policies established a highly regulated system for controlling the approval process and for identifying violations of these statutes, guidelines, and policies. Yet, notwithstanding these controls, we found serious abuses of national security letter authorities, which we described in our first NSL report. These included improperly obtaining consumer full credit reports, obtaining information beyond the time period specified in the NSLs, and issuing improper requests under the cited NSL statutes. Accordingly, contrary to the NSL Working Group's conclusions, we do not believe that existing controls are a sufficient basis upon which to rely in evaluating the need for additional privacy protections for NSL-derived information.

Second, as we elaborated earlier in this chapter and elsewhere in this report, while we agree that the FBI has made significant progress in addressing the findings in our first NSL report, we believe it is too soon to say that the FBI has rectified all of the problems we identified. Moreover, we believe it is too early to fully assess whether the new systems and controls developed by the FBI and the Department (including mandatory NSL training, the creation of the new NSL data system, the establishment of the OIC, and the NSD's national security reviews) will eliminate fully the improper or illegal uses of NSLs that we and the FBI have identified. Therefore, we believe the NSL Working Group should not base its recommendations on new and untested measures, some of which have only recently been implemented, some that are not yet implemented, and none of which have been evaluated by internal or external evaluators.

Third, the NSL Working Group's proposal does not explain the basis for two of its major conclusions. First, it does not explain how the new FBI data system for tracking issuance of NSLs relates to the principal FBI databases that store NSL-derived information. The memorandum does not explain how the "structured storage of information and NSL information can be segregated in the database" and the reasons for its conclusion that "individual tagging, as that term is commonly understood . . . did not provide any measurable value for privacy protections at this time." Second, the memorandum does not explain what options, including use of "meta

tags," the NSL Working Group considered and rejected or the basis for its conclusion that such measures would "place an undue burden" on the operation of NSLs. In later discussions, the Privacy Officer indicated that these matters would be more fully explained in the revised NSL Working Group report and recommendations.

Fourth, we are concerned that the NSL Working Group's proposed standard for uploading and retaining NSL-derived financial and credit information provides no meaningful constraint and requires no balancing of privacy interests against genuine investigative needs. The NSL Working Group's proposal would allow any information that a Special Agent believes "contributes" to an investigation to be uploaded and retained. As described by the NSL Working Group, it is difficult to conceive of responsive information that a Special Agent could not find "contributes" to an investigation in some way. Consequently, we believe the standard is so broad as to be meaningless. When we discussed the standard with the Privacy Officer, the Privacy Officer stated that the standard was intended to be limiting, although he stated that the August 17 memorandum did not provide appropriate clarity to ensure that the intended protections were real and not illusory.

Fifth, we are concerned that the NSL Working Group did not sufficiently assess whether to establish any time limits on the retention of NSL-derived data, sufficiently explain its reasoning for its conclusion, or at least consider more modest measures such as requiring that information derived from NSLs be reviewed during annual case reviews, when cases are closed, or after a reasonable period following the closing of investigations (for example, 3 or 5 years after closure). While we understand the NSL Working Group's rationale regarding the difficulty in predicting at a fixed point in time the investigative value of certain information, we are not convinced from the analysis contained in the NSL Working Group's memorandum that measures short of retention for 30 years are not feasible or workable. In particular, we do not find the NSL Working Group protocols sufficiently protective of the privacy interests of individuals who have been determined not to be of investigative interest.

For example, according to OIG interviews with FBI Special Agents, a primary use of NSLs is to close leads and eliminate suspects. Yet, information from NSLs for which the primary investigative value is to eliminate a suspect or close a lead falls within the NSL Working Group's broad definition of information having "investigative value" and may be uploaded and retained for many years. Under this approach, information related to individuals determined not to be of interest or concern to law enforcement also would be retained on the chance that the information could become relevant in the future. However, the argument that large amounts of data from NSLs that eliminated a suspect or closed leads should

be retained for many years because it *may* not be available in the future should be weighed against the individual's privacy interests. It is not clear that the NSL Working Group did this, and we do not believe it adequately explained its reasoning for rejecting alternatives other than the FBI's general retention policy regarding investigative information. In light of the vast amounts of digital information that the FBI can collect on communication, financial, and credit transactions, we believe the NSL Working Group did not give sufficient weight to the valid privacy interests that weigh against retention and accessibility of such data for 30 years. We believe the NSL Working Group should reconsider this significant concern when it reconvenes.

For the above reasons, we believe the NSL Working Group should reconsider its reasoning and conclusions that there should be no periodic review of data to determine whether the investigative value overcomes reasonable privacy interests. While we acknowledge that in many, and perhaps most, instances under such a review, the Special Agent or other official reviewing the case file may determine that the data should be retained, we believe that determination should be made only after a considered judgment rather than by application of a low standard that almost always will result in retention.

We also believe that the NSL Working Group should reconsider its proposal to allow unlimited uploading and retention of electronic communication transactional data regardless of its investigative value. We understand that information derived from ECPA NSLs must be uploaded into appropriate databases for link analysis and other examination to determine if it has investigative value. However, we are concerned that the NSL Working Group did not adequately consider or explain why it rejected a proposal that the FBI remove information that, upon analysis, is determined to have no investigative value after some reasonable period of time.

We also are not convinced by the NSL Working Group's initial assessment that the reduced privacy concerns associated with electronic communication transactional data, as compared with financial or credit data, justify rejection of any limits on uploading all responsive information. To the contrary, we believe that the volume of electronic communication transactional data collected, as well as the wide accessibility of that data, should be given more weight in balancing the need for additional privacy protections. As we describe elsewhere in this report, the vast majority of the FBI's NSLs are requests for electronic communication records under the ECPA. Further, much of the information in FBI databases is periodically transferred to the Investigative Data Warehouse. According to the FBI, the Investigative Data Warehouse contains data from 53 different sources and is

available to over 13,000 Special Agents, analysts, and law enforcement partners around the world.[42] Consequently, the Working Group should identify ways to establish meaningful controls to ensure that NSL-derived electronic communication transactional data, including information that has no identified investigative value, is not made widely available to the world-wide law enforcement community.

In sum, we believe it was premature for the NSL Working Group to conclude that current mechanisms to control the use and retention of NSL-derived information are adequate to protect the privacy and civil liberties of U.S. citizens. The NSL Working Group's preliminary conclusions are based in part on corrective measures that have not been fully implemented or demonstrated to be effective. We therefore believe that the NSL Working Group's recommendations related to the retention of NSL-derived information require further examination and explanation regarding how to balance the legitimate privacy interests of individuals against potential investigative needs. The NSL Working Group should consider whether and how to extend additional privacy safeguards to data obtained in response to the thousands of NSL requests issued each year that result in the collection of data on how U.S. citizens communicate, bank, and spend their money.

IV. OIG Conclusions and Recommendations

In conclusion, we believe the FBI and the Department have made significant progress in implementing the recommendations from our first NSL report and in adopting other corrective actions to address problems we and the FBI identified in the use of national security letters. We also found that the FBI has devoted significant energy, time, and 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.

For example, the FBI Director and Deputy Director have underscored the significance of the OIG's findings with senior Headquarters officials, SACs, and other personnel throughout the ranks of the FBI; stressed that compliance with NSL authorities is a major priority; and emphasized that personnel involved in drafting, reviewing, and approving NSLs will be held accountable for infractions. The Deputy Director and the General Counsel have reinforced these messages with SACs and CDCs. The FBI also has

---

[42] Federal Bureau of Investigation, "By the Numbers – FBI Transformation Since 2001," September 6, 2006, http://www.fbi.gov/page2/september 06/numbers090606.htm (accessed November 30, 2007).

generated comprehensive legal guidance on use of NSLs; provided mandatory NSL training to Assistant Special Agents in Charge, Supervisory Special Agents, Special Agents, and Intelligence Analysts; underscored the responsibility of CDCs in reviewing and approving NSLs and of case agents in ensuring that NSLs do not generate unauthorized records; and developed enhanced information technology tools that should facilitate the preparation of NSLs, reduce or eliminate errors, and improve the accuracy of congressional and public reporting on NSL usage. We believe that these and other steps taken in the last year underscore the FBI's commitment to addressing the problems we identified in our first NSL report.

The FBI's efforts to promote better compliance with NSL authorities also have been enhanced by other FBI initiatives and by the national security reviews conducted by the NSD and the FBI. The information developed from the FBI's 2007 NSL audits and the NSD's national security reviews is also likely to provide additional insights into problem areas and form the basis for additional guidance and compliance measures.

However, because only a year has passed since the OIG's first NSL report was released and some measures are not fully implemented, we also believe it is too early to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with the uses of NSLs that we and the FBI have identified. We believe the FBI must implement all of our recommendations in the first NSL report, demonstrate sustained commitment to the steps it has taken and committed to take to improve compliance, implement additional recommendations in this second report, consider additional measures to enhance privacy protections for NSL-derived information, and remain vigilant in holding FBI personnel accountable for properly preparing and approving NSLs and for handling responsive records appropriately.

In addition to the steps taken to date to address the recommendations in our first NSL report, we recommend that the FBI:

1. Create blank mandatory fields in the database supporting the NSL data system for entering the U.S. person/non-U.S. person status of the targets of NSLs and for entering the number of NSL requests in order to prevent inaccuracies that may otherwise result from the current default settings.

2. Implement measures to verify the accuracy of data entry into the new NSL data system by including periodic reviews of a sample of NSLs in the database to ensure that the training provided on data entry to the support staff of the FBI OGC National Security Law Branch (NSLB), other Headquarters divisions, and field personnel is successfully applied in practice and has reduced or eliminated data entry errors. These periodic

reviews should also draw upon resources available from the FBI Inspection Division and the FBI's new Office of Integrity and Compliance (OIC).

3. Implement measures to verify that data requested in NSLs is checked against serialized source documents to verify that the data extracted from the source document and used in the NSL (such as the telephone number or e-mail address) is accurately recorded on the NSL and the approval EC.

4. Regularly monitor the preparation of NSL-related documents and the handling of NSL-derived information with periodic reviews and inspections. This includes 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.

5. Assign NSLB attorneys to participate in pertinent meetings of operational and operational support units in the Counterterrorism and Counterintelligence Divisions.

6. Consider increasing the staffing level of the OIC so that it can develop the sufficient skills, knowledge, and independence to lead or directly carry out critical elements of the OIC's work.

We also recommend that the Department:

7. Direct that the NSL Working Group, with the FBI's and the NSD's participation, re-examine measures for (a) addressing the privacy interests associated with NSL-derived information, including the benefits and feasibility of labeling or tagging NSL-derived information, and (b) minimizing the retention and dissemination of such information.

CHAPTER THREE:
THE FBI'S 2007 REVIEWS OF NATIONAL SECURITY LETTERS IN RESPONSE TO THE OIG'S FIRST NSL REPORT

In this chapter, we describe additional efforts undertaken by the FBI in response to the OIG's 2007 report to review the FBI's compliance with statutes, guidelines, and internal policies governing the use of national security letters. Section I describes three FBI reviews of NSLs conducted in 2007 in response to the OIG's findings. These three FBI reviews were undertaken to assess the extent of the errors in NSL usage. The FBI conducted: (1) a review of NSLs issued by FBI field offices from a random sample of 10 percent of all national security investigations active at any time from 2003 through 2006; (2) a separate review of 10 percent of NSLs issued by Headquarters divisions during the same period; and (3) a review of NSLs issued in counterintelligence investigations pursuant to the *Fair Credit Reporting Act* (FCRA) from 2002 through 2006.

The OIG analyzed the results of these three reviews to assess their methodology and accuracy. Section II describes the results of the OIG's analysis.

The FBI's reviews were initiated soon after the issuance of the OIG's first NSL report in March 2007. In that report, the OIG had examined a judgmental sample of 293 NSLs from 77 national security investigation case files. In our sample, we identified 22 NSL-related possible intelligence violations, which represented a possible intelligence violation rate of 7.5 percent.[43] These errors included both improper requests from the FBI and unauthorized collections due to third party errors.

As discussed later in this chapter, the findings of the FBI's three NSL reviews generally confirmed the OIG's findings as to the types of errors made by FBI agents in their use of NSL authorities as well as the unauthorized collections caused by third parties that provided the FBI with information that was not requested. Current FBI policy requires that substantive errors in the use of NSL authorities by FBI personnel as well as errors caused by third parties resulting in overproduction of information to the FBI be reported to the FBI OGC and the FBI Inspection Division as potential Intelligence Oversight Board (IOB) violations (PIOBs). The FBI OGC reviews these reports and determines if the FBI has reason to believe that such conduct "may be unlawful or contrary to Executive Order or Presidential Directive," the IOB's reporting standard under Executive Order 12863. Although the types of

[43] The FBI OGC concluded that only 5 of the 22 matters identified by the OIG's first NSL report as possible intelligence violations should be reported to the IOB.

possible IOB violations identified by the OIG in our first NSL report and in the FBI's NSL reviews were similar, the FBI's field review of a larger sample, [redacted] case files, found a higher overall possible violation rate (9.43 percent) than the OIG found in its sample (7.5 percent).[44]

However, when we analyzed the FBI's 10-percent field office review, the OIG identified additional possible intelligence violations missed by the FBI. Moreover, inspectors were unable to locate records obtained in response to 6.8 percent of the NSLs selected for the field review.[45] Consequently, we believe that the rate of possible violations identified by the FBI in its 2007 field review is still understated, and therefore the FBI's field review does not provide a fully reliable baseline from which to measure improvement in compliance with NSL authorities in the future.

The OIG's review also found that the FBI reclassified as "administrative errors" some issues that initially were reported as possible intelligence violations during the field review. For some of these deficiencies, we are concerned that use of the phrase "administrative error" appears to understate the severity of the possible violation.

The FBI's 2007 reviews also identified two issues involving the use of NSLs that previously had not been fully addressed by the FBI. The FBI's reviews determined that: (1) FBI field offices received and retained Social Security Numbers and date of birth information in response to NSLs seeking subscriber information pursuant to the *Electronic Communications Privacy Act* (ECPA), even though this information was not requested in the NSLs; and (2) field offices and Headquarters operating divisions were often unable to locate records obtained in response to NSLs.

The FBI's 2007 reviews further demonstrated that the FBI's mechanism for identifying and self-reporting possible intelligence violations had been ineffective in the years since enactment of the Patriot Act in October 2001.[46]

---

[44] The FBI used a statistically valid sample that allowed its results to be projected to the universe of all NSLs issued by the FBI during the 2003 through 2006 review period. In our first NSL report, the OIG used a judgmental sample, and the results could not be statistically projected to the universe of all NSLs issued during the review period.

[45] The problems locating responsive records likewise affected the FBI's other reviews: records provided in response to 28 percent of NSLs examined in the Headquarters review were not initially located, and, in the FCRA review, 13 of the 56 field offices (23 percent) reported being unable to locate responsive records for 1 or more FCRA NSLs.

[46] The term "USA PATRIOT Act" is an acronym for the *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of* (Cont'd.)

In sum, we credit the FBI for using a reasonably sound methodology in conducting its reviews of NSL activities, for committing significant resources to the reviews, and for making the examination and analysis of the results a high priority. Its reviews confirmed the problems that the OIG's first NSL report identified. Although our analysis of the FBI's field and Headquarters reviews shows that the FBI was not able to ascertain the full extent of the possible violations of NSL authorities in national security investigations, the OIG nonetheless believes that the results of the FBI's reviews can help guide the corrective action that the FBI is implementing to enhance compliance with NSL authorities. These reviews again demonstrate that the additional remedial measures being implemented by the FBI are necessary and should remain a priority.

In the following sections, we discuss in more detail the FBI's 2007 reviews and our analysis of them.

I. The FBI's 2007 Reviews of National Security Letters

In this section, we examine the methodology and findings of three reviews conducted in 2007 by the FBI's Inspection Division in response to the OIG's first NSL report: (1) a review of NSLs issued by FBI field offices from a random sample of 10 percent of all national security investigations active at any time from 2003 through 2006; (2) a separate review of 10 percent of NSLs issued by Headquarters divisions during the same period; and (3) a review of NSLs issued in all counterintelligence investigations pursuant to the FCRA from 2002 through 2006.

A. The FBI's 2007 Field Review of National Security Letters

In response to the OIG's first NSL report, the FBI conducted a special review to assess whether FBI field offices complied with NSL statutes, Attorney General Guidelines, and internal FBI policies governing the use of NSLs and whether certain field offices had higher than average PIOB violation rates. The FBI assigned a large number of senior inspectors to conduct the reviews quickly, and the FBI made the review and analysis of the results a high priority. The FBI used a statistically valid sample and audit methodology that allowed its results to be projected beyond the sample of NSLs it reviewed to the universe of NSLs issued by the FBI during the review period.

2001, Pub. L. No. 107-56, 115 Stat. 272 (2001). It is commonly referred to as "the Patriot Act."

1. Methodology of the FBI's 2007 Field Review

To conduct its field review, the FBI selected a random sample of 10 percent of the case files in the three types of investigations in which NSLs may lawfully be issued: counterterrorism, counterintelligence, and foreign computer intrusion cyber investigations. The FBI determined that [redacted] of these types of investigations were active at any time between January 1, 2003, and December 31, 2006, and randomly selected [redacted] case files for review.[47] The FBI assigned 170 inspectors to review the case files at 56 field offices over a 5-day period (March 16, 2007, to March 20, 2007). The inspectors were instructed to review every NSL and related document in each selected file to determine if any possible intelligence violations occurred. When the review was completed, the inspectors had reviewed 7,863 NSLs issued during the 4 years covered by the review.[48]

Because many of the inspectors conducting the field review had no training or experience in issuing NSLs or with national security investigations, the FBI provided training and guidance on conducting the review. Inspection Division supervisors and FBI OGC attorneys told us that they repeatedly instructed the inspectors to "err on the side of over-reporting" possible intelligence violations even if they did not involve an NSL-related violation.[49] Also, the Chief Division Counsels (CDC) at each

---

[47] The FBI sample was proportional by case type (counterterrorism, counterintelligence, and cyber investigations) and field office. The [redacted] cases included investigations for which the FBI OGC NSL tracking database showed that one or more NSLs had been issued as well as investigations in which the database showed no NSLs. The inspectors found NSLs in [redacted] of the case files. The number of case files reviewed at each field office ranged from [redacted] in the El Paso and Anchorage field offices to [redacted] in the New York field office. The number of NSLs reviewed in each field office ranged from [redacted] in Knoxville to [redacted] in the Washington, D.C., field offices. The FBI's random sample included [redacted] cases that were designated as FBI Headquarters investigations. There were 16 NSLs within these case files, and these NSLs were reviewed as a part of the FBI's field audit, not the Headquarters audit.

[48] However, the FBI inspectors could not locate records in response to 532 NSLs, and 1,175 NSLs (including these 532) were not fully reviewed because the inspectors could not find all relevant documents (approval electronic communication (EC)), NSL, and responsive records) or were unable to make a determination as to whether a possible intelligence violation had occurred. We did not include in our calculations of the unauthorized collection portion of the PIOB error rates NSLs for which responsive records could not be located.

[49] Inspection Division personnel supervising the audit told us that they instructed the inspectors not to search case files for infractions unrelated to national security letter authorities (for example, if investigative activity unrelated to NSLs occurred after authorization for the investigation had lapsed). However, if they encountered such violations, referred to as "other" reportable possible intelligence violations, they were instructed to document the possible violations.

field office were made available to answer questions from the inspectors while they were on site at the field offices.

When the inspectors noted possible violations during the field review, they were instructed to give a paper copy of the NSL, the associated approval memorandum (referred to as the approval Electronic Communication or EC), and a PIOB violation form to the field office's CDC. The inspectors also transmitted the results of their reviews to the Inspection Division on a daily basis. The Inspection Division aggregated this information into a consolidated database for analysis.

For each possible intelligence violation the FBI inspectors identified and reported to the Inspection Division the CDCs were instructed to make a preliminary decision as to whether the matter should be reported to the FBI OGC as a possible intelligence violation based on guidance issued by the FBI OGC in November 2006. These preliminary decisions were forwarded to the Inspection Division. Regardless of these initial decisions, the CDCs were instructed to then make an "official" determination in writing and forward those decisions, along with all NSL-related documentation, to the FBI OGC.[50] As of February 2008, the FBI OGC was in the process of adjudicating which matters in fact were reportable to the FBI OGC and determining which matters should be reported to the IOB.

2. The FBI's Post-Field Work Analysis

Upon completion of the field review, supervisors in the Inspection Division analyzed the results reported by the inspectors to identify the extent of the NSL-related possible intelligence violations in each FBI field office. During their preliminary review of the results, the supervisors discovered that:

- some information entered by the inspectors was incomplete or contradictory;
- some forms reported possible intelligence violations that the supervisors did not believe rose to the level of being reportable; and
- certain field offices had significantly lower rates of possible intelligence violations compared with other field offices.

---

[50] As of December 4, 2007, an Inspection Division supervisor told us that all 56 CDCs had forwarded documentation of the reported possible intelligence violations to the FBI OGC. However, some CDCs did not make official determinations of whether the matters reported to them were possible intelligence violations; instead, these CDCs merely forwarded the facts and documents related to the potential intelligence violations to the FBI OGC for its review and determination.

To resolve contradictions in information submitted by inspectors and determine whether possible intelligence violations had occurred, Inspection Division supervisors performed what they termed a "scrubbing process" during which they examined each form to identify and resolve any discrepancies. Specifically, the supervisors reviewed the PIOB forms to determine why some forms were submitted without identifying a possible intelligence violation and to resolve contradictions between possible violations noted and the inspectors' comments.

Simultaneously, the Inspection Division supervisors requested guidance from the FBI OGC regarding violations that the supervisors did not believe rose to the level of a possible intelligence violation, such as instances in which inspectors were unable to locate the signed copy of an NSL.[51] The FBI OGC agreed with the supervisors that certain types of errors noted by the inspectors did not constitute an NSL-related possible intelligence violation. Consequently, the FBI OGC attorneys created a list of 11 NSL-related infractions they termed "administrative errors." Table 3.1 provides a list of the infractions the FBI OGC deemed NSL-related administrative errors. Using the FBI OGC's list, the Inspection Division supervisors re-examined the entries on the PIOB forms and determined whether they were reportable NSL-related possible intelligence violations or administrative errors.

[51] As we reported in our first NSL report, FBI policy did not require retention of signed copies of NSLs. In March 2007, in response to the OIG's recommendations, the FBI directed that signed copies of NSLs must be retained in the investigative file to which the request relates. See Records Management Division, Federal Bureau of Investigation (FBI), electronic communication to all Divisions, Procedural and Operational Issuances, March 9, 2007. As described fully in Chapter Two of this report, FBI policy now requires that the NSL itself must be uploaded as an NSL document into the Automated Case Support (ACS) system. Id.

TABLE 3.1
NSL-Related Infractions Identified in the FBI's 2007 Field Review Later Classified by the FBI as "Administrative Errors"

Nature of NSL Infraction	Number of Infractions
Unable to locate NSL results/records submitted by the NSL recipient	532
Approval EC lacked detailed information on specific records requested compared with details in the NSL	433
Approval EC did not cite specific statutory authority for issuing the NSL	136
Unable to locate signed NSL	102
Unable to determine if the NSL was served	81
Unable to locate initialed/approval EC requesting issuance of NSL	71
Approval EC requesting issuance of NSL lacked appropriate approvals	50
Records requested in approval EC differed from records requested in the NSL	33
Statutory authority cited in the approval EC differed from the citation in the NSL	33
Error in typing/recording of NSL date	20
Error in typing/recording of approval EC date	7
Total	**1,498**

Finally, regarding the variation in PIOB violation rates between field offices, the Inspection Division supervisors were concerned that the inspectors who reported low PIOB violation rates for the field offices to which they were assigned may have missed possible intelligence violations. To determine whether that had occurred, the Inspection Division conducted follow-up visits to six field offices to re-review the files examined during the initial inspection. The supervisors' concerns proved correct. During the initial field visits, the inspectors had identified one NSL-related possible intelligence violation in these six offices. Inspectors assigned to the follow-up visits found 83 additional possible intelligence violations that were missed by the first inspection teams.

3. The FBI's Findings

After the Inspection Division supervisors completed the scrubbing process, they reported to the OIG that as of November 2007, they had identified 640 NSL-related possible intelligence violations in 634 NSLs.[52] These 640 matters included:

---

[52] The data presented below describing the 640 NSL violations is a summary of the initial decisions made by CDCs during the FBI's field review and does not reflect the final decisions that will be made by the FBI OGC. As we previously noted, as of February 2008 (Cont'd.)

- **Improper Authorizations.** Approximately 6 percent involved violations of internal FBI policy designed to ensure appropriate supervisory and legal review. These included instances in which NSLs were issued from investigations that were inactive or had not been properly authorized, lacked documentation of predication, lacked documentation of required approvals, or did not document the relevance of the requested information to the underlying investigation in the approval ECs.
- **Improper Requests.** Approximately 4 percent involved NSLs that requested information the FBI was not authorized to request.
- **Unauthorized Collections.** The majority (90 percent) involved the receipt of records not requested in the NSL or the receipt of information not relevant to an FBI investigation.

"Unauthorized collections" is a phrase used by the FBI and the OIG to describe several circumstances in which the FBI receives information in response to NSLs that was not requested or was mistakenly requested. For example, many unauthorized collections occur due to errors on the part of NSL recipients when they provide more information than was requested (such as records for a longer period of time or records on additional persons). The FBI sometimes also refers to these matters as "over collections" or "overproductions." We refer to these as "initial third party errors" because, while the NSL recipient may initially have provided more information than requested, the FBI may or may not have compounded the initial error by using or uploading the information. Other unauthorized collections can result from FBI errors, such as when a typographical error in the telephone number or e-mail address results in the acquisition of data on the wrong person or e-mail address. When we present data on "unauthorized collections" in this report we note whether the infraction occurred due to initial third party error or FBI error.

Table 3.2 provides more specific information on the types of NSL-related possible intelligence violations identified during the FBI's field review and shows how many times each type occurred. In the table below and elsewhere in this report, we use the phrase "initial third party error" to describe a mistake initially attributable to the NSL recipient of providing more information than requested by the FBI. In some instances, FBI employees identified such overproductions and segregated the information,

---

the FBI OGC had not completed reviewing and adjudicating all of the possible intelligence violations identified during the FBI's field review. The FBI OGC will make the determination as to the types of potential intelligence violations that the field should report to the FBI OGC as well as the violations the FBI determines are reportable to the IOB.

rather than using it or uploading the information into FBI databases. However, we found that in all but 1 percent of the instances identified by the FBI's field review (4 of 557), FBI personnel failed to identify the improperly provided information and thereby failed to take required steps for sequestering the information from the case file and ensuring that the information was not used or uploaded into FBI databases.[53] Because these 553 matters were not identified by field agents or supervisors, they were not self-reported to the FBI OGC as required.

TABLE 3.2
Possible NSL-Related IOB Violations
Identified in the FBI's 2007 Field Review (2003 through 2006)

Category	Possible NSL-Related IOB Violation	Number	Percentage
Improper Authorizations (FBI error)	NSL issued with no authorized investigation (no case ever opened)	2	-
	NSL lacked predication or sufficient justification, or information sought not relevant to the investigation	5	-
	NSL issued in a preliminary investigation prior to January 16, 2003	0	-
	NSL issued in a preliminary investigation under FCRA between January 16, 2003, and December 31, 2003	2	-
	NSL lacked approval of Senior Executive Service official	28	-
	NSL requested before or after authorized period of investigation	3	-
	Total Improper Authorizations	**40**	**6.25%**
Improper Requests (FBI error)	NSL issued under FCRAv for a consumer full credit report in a counterintelligence case with no nexus to international terrorism	14	-
	NSL-requested information beyond the scope permissible by statute	10	-
	Total Improper Requests	**24**	**3.75%**

[53] As discussed in Chapter Seven, on August 1, 2007, the IOB directed the FBI OGC to report third party errors that are compounded by the FBI. After this direction, FBI OGC officials told us that they began evaluating third party errors to determine if the FBI compounded the errors by using the inappropriately provided information or uploading it into FBI databases. If the FBI compounded a third party error, FBI OGC officials told us they would report the matter to the IOB.

Category	Possible NSL-Related IOB Violation	Number	Percentage
Unauthorized Collections (FBI error or initial third party error)	The NSL recipient provided data in excess of the NSL request (initial third party error)	364	-
	The NSL recipient furnished records or information not requested in the NSL (initial third party error)	312	-
	NSL issued with typographical mistakes in names, addresses, telephone numbers, account numbers, etc. (FBI error)	19	-
	Note: The total of the three rows above must be adjusted to account for NSLs that had violations reported in more than one category	(119)	
	Total Unauthorized Collections	**576**	**90.00%**
	Total NSL PIOB Violations	**640**	**100.00%**

Note: We derived the percentage of violations by dividing the number of occurrences by 640, the total number of NSL-related PIOB violations.

As shown in Table 3.2, 576 of 640 (90 percent) possible intelligence violations were the result of the unauthorized collection of telephone or e-mail transactional records, financial records, and credit records pursuant to the ECPA, RFPA, and FCRA NSL statutes. These unauthorized collections occurred due to errors made either by NSL recipients (initial third party error) or by the FBI. For example, these included instances in which:

1. The NSL recipient erred by providing data in excess of the NSL request, such as providing information for a full billing cycle rather than providing records for the shorter period requested in the NSL.[54]

2. The NSL recipient erred by furnishing records or information not requested in the NSL, such as information on individuals who used a particular telephone number or e-mail address during dates before or after the subject of the FBI investigation.[55] Certain NSL recipients also produced Social Security Numbers and dates of birth in response to ECPA NSLs

[54] In May 2006, the FBI OGC approved use of a revised attachment for ECPA toll record NSLs that included information "which encompasses the billing cycle that is used with respect to the account(s) information requested" among the types of records that may be considered by the recipients to be "toll billing records."

[55] FBI OGC attorneys told us that if the date range in the NSL was reasonable when the NSL was issued, and the records received were within the date range of the NSL, the FBI OGC does not consider such records to be unauthorized collections.

seeking subscriber information, even though this information was not requested in the NSL.[56]

3. The FBI erred by requesting information on the wrong telephone number, e-mail account, or Internet Protocol address in the NSL due to FBI typographical errors.

4. Comparison of Findings in the FBI's 2007 NSL Field Review and the OIG's First NSL Report

The findings of the FBI's 2007 NSL field review were generally consistent with the OIG's findings in our March 2007 NSL report as to the types of errors made by FBI agents in their use of NSL authorities. Although the types of possible intelligence violations identified by the OIG and in the FBI's 2007 field review were similar, the FBI's review found a higher overall violation rate and a higher rate of errors attributable to third party unauthorized collections than the OIG found.

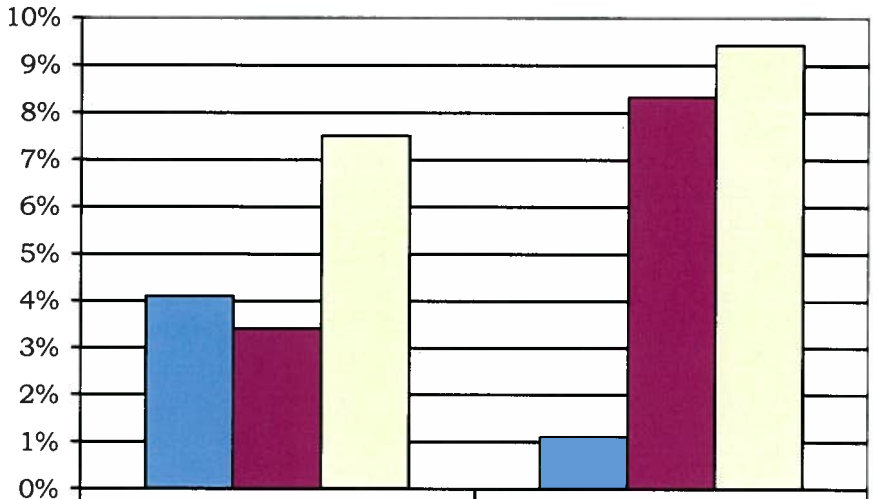
In the OIG's judgmental sample of 77 national security investigation case files maintained by 4 field offices, we identified 22 possible violations in the 293 NSLs we examined that we believed should have been reported to the FBI OGC.[57] Of those 22 violations, 10 involved unauthorized collections due to third party error. In its 2007 field review, FBI inspectors reviewed 6,688 NSLs for which all relevant NSL documents were available, (approval EC, NSL, and responsive records) and found 634 NSLs that contained 640 possible violations. Of those 640 violations, 557 involved unauthorized collections attributable to initial third party errors. A comparison of these findings for the two reporting periods is illustrated in Chart 3.1.

---

[56] As discussed in Chapter Two of this report, in August 2007 the FBI OGC requested a legal opinion from the Department's Office of Legal Counsel (OLC) on whether the FBI may lawfully retain Social Security Numbers and date of birth information provided to the FBI in response to NSLs seeking subscriber information pursuant to the *Electronic Communications Privacy Act* (ECPA), 18 U.S.C. § 2709(c). As of February 2008, the OLC had not issued its opinion.

[57] Following issuance of our first NSL report, the FBI OGC instructed pertinent field offices to report the 22 potential IOBs to the FBI OGC. The FBI OGC determined that only five were reportable to the IOB. The five matters that were reported to the IOB were issuance of an NSL without obtaining required approval to extend the investigation; issuance of an NSL for material that arguably constituted prohibited content; issuance of an NSL citing the ECPA NSL statute that requested the *Right to Financial Privacy Act* (RFPA) financial records associated with e-mail accounts; and issuance of two NSLs requesting consumer full credit reports pursuant to 15 U.S.C. § 1681v in a counterintelligence case with no international terrorism nexus.

CHART 3.1
Comparison of Possible NSL-Related IOB Violations Identified in the OIG's First NSL Report and the FBI's 2007 Field Review



	OIG NSL I (2003 - 2005)	FBI Field Review (2003 - 2006)
FBI NSL PIOBs	4.10%	1.10%
Third Party NSL PIOBs	3.41%	8.33%
Total NSL PIOB Rate	7.51%	9.43%

B. The FBI's 2007 Headquarters Review of NSLs

As a result of the OIG's findings in our first NSL report, the FBI Inspection Division also conducted a special review of NSLs issued by Headquarters divisions to determine the nature and extent of any problems associated with these NSLs. In this section, we describe the Inspection Division's review of NSLs issued by Headquarters divisions from 2003 through 2006, including the FBI's methodology, findings, and subsequent recommendations.

1. Background

In our first NSL report, the OIG found that FBI Headquarters personnel issued approximately 300 NSLs exclusively from control files rather than from investigative files. If NSLs are issued exclusively from control files, case agents and their supervisors cannot determine whether the requests are tied to substantive investigations that have established the required evidentiary predicate for issuing NSLs. Issuing NSLs from control files is contrary to internal FBI policies.

2. FBI Methodology

To determine the extent of NSL-related possible intelligence violations in FBI Headquarters divisions, in April and May 2007 the FBI Inspection Division reviewed a random sample of approximately 10 percent of 2,440 NSLs (249 were selected for review) issued between January 1, 2003, and December 31, 2006, by FBI Headquarters divisions.[58] The FBI searched the Automated Case Support (ACS) system to identify the universe of NSLs issued from Headquarters.[59] Once the universe of NSLs was identified and the sample was selected, the process used to conduct the Headquarters review was similar to that used for the field review: inspectors manually and electronically (through the ACS system) reviewed documentation, including the approval ECs, the NSLs, and information received in response to the NSLs for compliance with NSL statutes, Attorney General Guidelines, and internal FBI policies.

3. The FBI's Headquarters Findings

The Inspection Division's review of Headquarters-issued NSLs produced much higher violation rates than those the FBI reported in the field review. In total, the FBI inspectors identified 165 possible violations in the 249 Headquarters NSLs they reviewed. The 249 Headquarters NSLs were tied to 25 case files, of which 15 were investigative files and 10 were control files. The Headquarters review also identified a type of error – issuance of NSLs solely from control files – that was not identified in the FBI's field review and that accounted for a significant proportion of the possible intelligence violations. Over 50 percent (125) of the NSLs in the FBI's Headquarters review sample were issued exclusively from control files, in violation of internal FBI policy. As a result of these NSLs, the overall PIOB violation rate for Headquarters-issued NSLs was 71.5 percent, compared with a 9.4-percent violation rate in the FBI's field review.[60]

---

[58] The Inspection Division's review of the Headquarters-issued NSLs consisted of a 10-percent sample of NSLs issued from Headquarters. This was a different methodology than that used in the field review, which consisted of a review of all NSLs contained within the 10-percent sample of randomly selected national security investigation case files.

[59] The Inspection Division used a keyword search on approval ECs in the ACS system to identify its universe of NSLs. However, this search would have missed those NSLs issued without approval ECs. Additionally, the NSLs selected for the review of Headquarters' case files could not be identified by case file number through the ACS system because NSLs issued by Headquarters officials did not always have a case file associated with the NSLs.

[60] The FBI's Headquarters review found NSLs issued from control files because the FBI had not issued specific guidance on this issue until 2007. As discussed in our first NSL report, many of the NSLs issued from Headquarters control files related to classified

(Cont'd.)

Even if the 125 NSLs issued from control files are not included, the resulting violation rate of 22.4 percent would place Headquarters among those field offices having the highest violation rates. Only 3 of 56 field offices had higher violation rates than Headquarters.

Table 3.3 provides specific information on the types of possible violations found during the FBI's Headquarters review and identifies how many times each violation occurred.

TABLE 3.3
Possible NSL-Related IOB Violations Identified in the FBI's 2007 Headquarters Review (2003 through 2006)

Category	Number of Errors	Rate of Error
NSL issued from control file with no open investigation (FBI error)	125	50.2%
NSL lacked predication or sufficient justification, or information sought not relevant to the investigation (FBI error)	5	2.0%
NSL requested information beyond the scope permissible by statute (FBI error)	2	0.8%
NSL issued with typographical mistakes in names, addresses, telephone numbers, account numbers (FBI error)	1	0.6%
NSL recipients provided data in excess of the NSL request, or furnished records or information not requested in the NSLs (initial third party error)	32	17.9%*
Total	**165**	**71.5%**

*The rate of third party error is based only on the 179 NSLs for which inspectors were able to locate and review records obtained in response to the NSLs. When responsive information could not be located during the Headquarters review, the OIG eliminated those NSLs from the third party error rate calculation.

The FBI inspectors reviewing Headquarters-issued NSLs had greater difficulty locating signed copies of NSLs and records provided by NSL recipients than inspectors who reviewed NSLs during the field review. During the review of Headquarters-issued NSLs, inspectors were unable to locate signed copies of 225 of the 249 NSLs identified for the review and were unable to locate the records provided by the NSL recipients in response to 70 NSLs (28 percent).[61] In addition, the inspectors found 168 approval ECs that did not reference preliminary or full investigations, which made it

---

special projects. See NSL I, 98-103. The FBI Inspection Division reported that 88 of these 125 NSLs (70 percent) were generated from these classified special projects.

[61] At the time of the Headquarters review, responsive records could not be located. Inspection Division personnel told us that these records were later located in Headquarters closed files and were reviewed to determine if there were overcollection.

difficult to determine if the NSLs were issued from authorized investigations as required by the NSL statutes and the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines).

To address the deficiencies identified in its review of Headquarters-issued NSLs, the Inspection Division recommended that: (1) the Assistant Director for the Counterterrorism Division (CTD) perform a file review every 90 days of all Headquarters national security investigation case files to ensure NSL compliance, and (2) internal controls should be strengthened to ensure that each Headquarters NSL can be verified and associated with its responsive records. The Inspection Division also recommended that the Assistant Director for the CTD and the FBI General Counsel provide appropriate training to CTD personnel on the proper use of NSLs and that the Assistant Director for the CTD take action to facilitate the appropriate reporting of possible NSL-related intelligence violations to the FBI OGC. As of October 2007, a draft e-mail had been prepared for the signature of the Assistant Director instructing the FBI Headquarters divisions to review the possible intelligence violations identified by the Inspection Division's review of Headquarters-issued NSLs. The Headquarters division personnel were also instructed to provide a written response to the Inspection Division with specific information on each possible intelligence violation, stating whether they agreed that a possible violation existed and to report those findings to the Internal Investigation Section, to the CTD, and to the FBI OGC.

C. The FBI's Review of FCRA NSLs Seeking Consumer Full Credit Reports in Counterintelligence Investigations

In response to the findings of the OIG in the first NSL report, the FBI recognized that some of its employees did not understand that a FCRA NSL could not be used to obtain a consumer full credit report in a counterintelligence investigation that does not have a nexus to international terrorism. Accordingly, to ensure that no such credit reports were in its files, the FBI ordered a review of all FCRA NSLs that had been issued in counterintelligence matters from January 1, 2002 through December 31, 2006, in all 56 field offices. In this section, we provide a brief summary of the OIG's findings in our first NSL report on the FBI's use of FCRA NSLs from 2003 through 2005. We then describe the results of the FBI's 2007 review of FCRA NSLs issued in counterintelligence investigations during the 5-year period the FBI reviewed.

1. The OIG's Findings on FCRA NSLs in Our First NSL Report

In our first NSL report, the OIG examined the potential intelligence violations self-reported by FBI personnel to the FBI OGC in 2003 through

2005 and found that only one involved an improper request for a consumer full credit report in a counterintelligence investigation with no nexus to international terrorism.[62] This matter subsequently was reported to the IOB.[63] However, during our review of investigative case files in four FBI field offices, we identified two additional improper requests for consumer full credit reports in counterintelligence investigations. These improper requests were not reported to the FBI OGC pursuant to the mandatory self-reporting requirement.[64] After examining these two additional matters, the FBI reported both to the IOB in 2007.

In addition to noting the potential intelligence violations involving use of FCRA NSLs summarized above, we found in our first NSL report that FBI field personnel sometimes confused the two NSL authorities under the FCRA. Although the National Security Law Branch (NSLB) attorneys sent periodic guidance and e-mails to all CDCs to clarify the distinctions between the two FCRA NSLs, we found that problems and confusion persisted. Accordingly, we recommended that the FBI issue additional guidance to field offices to clarify the two authorities and improve the identification of possible intelligence violations arising from the use of FCRA NSLs.[65]

2. The FBI's 2007 Review of FCRA NSLs

a. Directive to the Field

On March 5, 2007, the FBI's Executive Assistant Director for the National Security Branch (EAD NSB) directed the FBI's 56 field offices and the Counterintelligence Division to review all FCRA NSLs issued from January 1, 2002, through December 31, 2006, in counterintelligence investigations.[66] The purpose of the review was to determine whether any of

---

[62] The FCRA was enacted in 1970 to protect personal information collected by credit reporting agencies. In 2001, the Patriot Act amended the FCRA to add a new national security letter authority, referred to as FCRAv NSLs, which authorizes the FBI to obtain a credit reporting agency's reports and "all other" consumer information in its files. Thus, the FBI can now obtain full credit reports on individuals during national security investigations upon certification that the information is "necessary for" the FBI's "investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism . . . ." See NSL I, 14-15.

[63] Id. at 70-72.

[64] Id. at 79-81.

[65] We discuss this guidance in Chapter Two of this report in connection with Recommendation 4 in our first NSL report.

[66] National Security Branch, FBI, electronic communication to all Field Offices and Counterintelligence, Guidance on Use of Fair Credit Reporting Act NSLs in Counterintelligence Investigations; Review of Fair Credit Reporting Act NSLs Issued in CY 2006 in Counterintelligence Investigations, March 5, 2007. In response to the directive (Cont'd.)

these NSLs requested consumer full credit reports or resulted in the receipt of such reports in violation of the NSL statutes, Attorney General Guidelines, or internal FBI policies. The directive stated that if any such reports were requested or obtained in the absence of the required nexus to international terrorism, the incidents were to be reported to the FBI OGC as possible intelligence violations regardless of whether the information was requested by the FBI or was erroneously produced by the credit reporting agency. The directive also stated that the consumer full credit reports must be sequestered with the field office's CDC pending the issuance of the FBI OGC's opinion as to whether the matter should be sent to the IOB.[67]

b. Summary of Findings

In response to the directive, 41 FBI field offices reported that they had identified one or more FCRA NSLs that constituted improper requests or resulted in unauthorized collections. The two types of unauthorized collections included instances in which the response to the FCRA request exceeded the scope of the request by providing the following:

- The NSL requested FCRAu(a) financial institution-identifying information or FCRAu(b) consumer-identifying information but the response included a consumer full credit report.
- The NSL requested FCRAu(b) consumer-identifying information but the response included financial institution-identifying information.

Thirteen of the 56 field offices (23 percent) reported being unable to locate the results of at least 1 FCRA NSL. One office reported being unable to locate the results of 97 FCRA NSLs. Table 3.4 summarizes the potential violations reported by the FBI field offices to the FBI OGC in response to the EAD NSB's directive. Each type of violation is described further in the following section.

---

from the EAD NSB, each of the 56 field offices reported their results via EC. These are the documents the OIG reviewed in order to perform its analysis of the results of the FBI's FCRA NSL review. The Counterintelligence Division responded that it had not issued any FCRA NSLs during the review period.

[67] Id.

TABLE 3.4
Possible FCRA IOB Violations Identified in the FBI's 2007 Review of NSLs Issued in Counterintelligence Investigations (2002 through 2006)

FCRA PIOBs Reported by FBI Field Offices	No. of Field Offices	No. of NSLs	No. of Consumer Full Credit Reports Provided to the FBI	No. of PIOBs Previously Self-Reported
NSL requests for consumer full credit reports in counterintelligence investigations with no nexus to international terrorism (FBI error)	11	33	29	2
NSL requests for limited credit information for which consumer full credit reports were provided (initial third party error)	35	233	233	6
NSL requests for consumer-identifying information for which financial institution-identifying information was provided (initial third party error)	1	1	N/A	0

c. Improper Requests

Of the 56 FBI field offices, 11 reported that they had issued a total of 33 FCRAv NSLs in counterintelligence investigations with no nexus to international terrorism.[68] However, in one instance, a case agent and supervisor thought that the original FCRAv request was justified because the investigation later developed a nexus to international terrorism.[69] In another four instances, the requesting field offices did not receive the consumer full credit reports that they had improperly requested. Consequently, of the 33 FCRAv NSLs reported by the field offices, 33 were improper requests and 29 were improper requests for which the FBI obtained unauthorized information (consumer full credit reports). Of the 33 improper FCRAv NSLs identified in the review, only 2 had previously been reported to the FBI OGC pursuant to the mandatory self-reporting requirement.

---

[68] Three of these 33 FCRAv NSLs contained a reference to the FCRAu NSL statute, but the text of the NSL requested "credit reports" or "all information in the file." The FBI categorized these as improper requests.

[69] FBI OGC attorneys told the OIG that the nexus to international terrorism must exist at the time the NSL is issued.

d. Unauthorized Collections

Thirty-five of the FBI's 56 field offices reported that they had obtained unauthorized collections in response to NSLs seeking limited credit information pursuant to 15 U.S.C. § 1681u(a). These field offices had issued a total of 233 FCRAu NSLs requesting limited credit information, in response to which credit reporting agencies had produced consumer full credit reports.[70] During the review period, the FBI had issued a total of [redacted] FCRAu NSLs of which [redacted] were issued in counterintelligence cases. Thus, [redacted] percent of these [redacted] NSLs resulted in unauthorized collections. Of these 233 unauthorized collections, only 6 (3 percent) had previously been reported to the FBI OGC pursuant to the mandatory self-reporting requirement.

In another type of unauthorized collection, one FBI field office reported that it had obtained financial institution-identifying information (permissible in response to 15 U.S.C. § 1681u(a) NSLs) in response to an NSL seeking consumer-identifying information pursuant to 15 U.S.C. § 1681u(b).[71]

II. The OIG's Analysis of the FBI's 2007 NSL Reviews

In this section, we provide the OIG's analysis of the three NSL reviews conducted by the FBI in 2007, described above.

A. The OIG's Verification of the FBI's 2007 Field Review of NSLs

To assess the accuracy of the FBI's field review, the OIG visited three field offices and re-examined case files that had been reviewed by FBI inspectors during the field review. We found that the FBI's field review used a sound sampling methodology but that FBI inspectors missed a significant number of NSL-related possible intelligence violations as they were reviewing the case files, thereby understating the actual rate of possible

---

[70] Among the 233 unauthorized collections was one instance in which the case agent could easily read the text of the consumer full credit report, even though the credit reporting agency attempted to redact this information. Moreover, the case agent relied on the poorly redacted information received from the credit reporting agency to later issue two NSLs seeking financial information pursuant to the *Right to Financial Privacy Act* (RFPA) NSL statute.

[71] The FCRAu(a) NSL statute, 15 U.S.C. § 1681u(a), authorizes the FBI to obtain the names and addresses of all financial institutions at which a consumer maintains or has maintained an account. The FCRAu(b) NSL statute, 15 U.S.C. § 1681u(b), authorizes the FBI to obtain the consumer's name, address, former addresses, places of employment, or former places of employment.

intelligence violations. In this section, we describe the methodology of our review, our findings, and our analysis.

1. The OIG's Methodology

The OIG reviewed a judgmental sample of the case files examined by FBI inspectors at three field offices during the FBI's March 2007 field review. The OIG's review was not designed to question the judgments of the CDCs or the Inspection Division determinations regarding whether violations identified by the inspectors were reportable to the IOB. Instead, our objective was to determine if the inspectors had identified all of the NSL-related possible intelligence violations in the files. Therefore, in selecting our sample for review, the OIG did not include any NSLs that were previously identified by the FBI's inspectors as containing possible NSL-related intelligence violations.

The three field offices we selected for our review had an average NSL violation rate below the FBI field review's overall 9.43-percent violation rate.[72] Just as the Inspection Division did when selecting its field offices for re-visits, the OIG selected field offices with NSL violation rates below the overall average to test the assumption that these lower-than-average rates were the result of FBI inspectors missing violations in some of the NSLs they reviewed.

Using a judgmental sample, the OIG selected 15 case files in each of the 3 field offices, and from those files identified up to 60 NSLs in each field office to review.[73] The OIG selected case files that contained possible intelligence violations previously identified by the FBI inspectors during their review (and later confirmed by the CDCs), as well as case files in which no possible intelligence violations were identified by the inspectors. We reviewed the NSLs using the same criteria that the FBI inspectors were instructed to use during the FBI field review.

2. Findings of the OIG's Review

The OIG's review found that the FBI's field review did not identify a significant number of NSL-related possible intelligence violations. In the 42

---

[72] At the 3 field offices we visited, the FBI inspectors had previously reviewed a total of 1,114 NSLs and identified 33 NSL-related possible intelligence violations in those NSLs, for a PIOB violation rate of 2.96 percent for the 3 offices. Individually, the PIOB violation rates for the three offices were 2.56 percent, 2.47 percent, and 6.30 percent.

[73] The OIG selected sufficient samples to allow for cases that were not available for review. We ultimately reviewed 13 files in Field Office 1, 14 files in Field Office 2, and 15 files in Field Office 3, for a total of 42 files. From those 42 files, we reviewed a total of 169 different NSLs.

case files re-examined by the OIG, the FBI's inspectors had previously reviewed 396 NSLs and identified 13 possible intelligence violations, for a violation rate of 3.28 percent. The OIG re-examined 169 of the NSLs in which the FBI inspectors had identified no possible intelligence violations, and we identified an additional 15 possible intelligence violations, for a violation rate of 8.88 percent.[74] Overall, the violation rate identified by the OIG was almost 3 times higher than the violation rate found by the FBI in these 42 case files. Table 3.5 describes the type and number of violations identified by the OIG in these case files. As noted above, we use the phrase "initial third party error" to describe instances in which the NSL recipient provided records beyond those requested in the NSLs. However, the FBI may at times have compounded the initial third party error by using or uploading the improperly provided information.

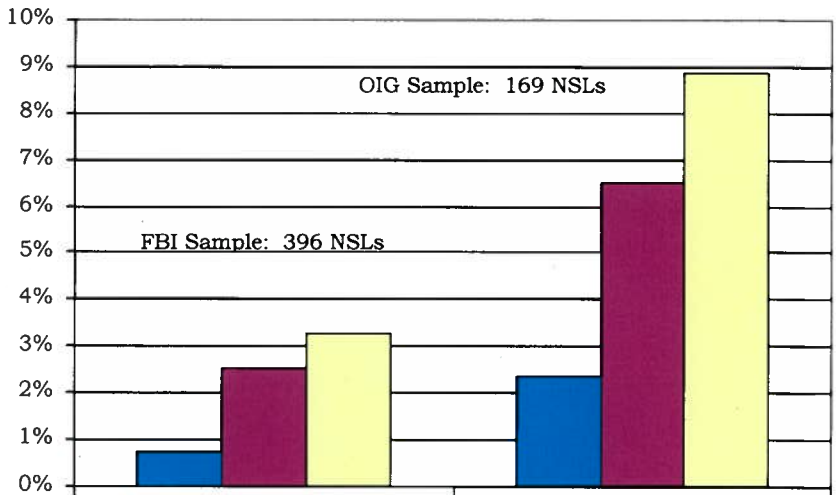
TABLE 3.5
Possible NSL-Related IOB Violations Identified by the OIG Not Identified by FBI Inspectors at Three Field Offices During the FBI's 2007 Field Review

Category	NSL-Related PIOB Violations	Number
Improper Authorization	NSL lacked predication, sufficient justification, or documentation of relevance to the investigation (FBI error)	2
	Subtotal	**2**
Unauthorized Collection	NSL issued with typographical mistakes in names, addresses, telephone numbers, account numbers, etc. (FBI error)	2
	NSL resulted in collection of data requested in the NSL but for a longer (or different) period than was designated in the NSL (initial third party error)	6
	NSL resulted in collection of data not requested in the NSL or which was not relevant to the investigation (initial third party error)	5
	Subtotal	**13**
	Total	**15**

Chart 3.2 compares the error rates identified in the 42 case files at the 3 field offices visited by both the FBI and the OIG. The chart illustrates the rate of errors attributable to the FBI or initial third party error.

[74] The OIG was unable to locate records responsive to 15 of the 169 NSLs we reviewed. The 8.88 percent violation rate therefore did not include possible intelligence violations that may have resulted from records obtained in response to these 15 NSLs.

CHART 3.2
Comparison of Possible NSL-Related IOB Violations Identified by the FBI and the OIG (by category) in NSLs Reviewed in Three Field Offices



	FBI	OIG
PIOB Rate Due to FBI Error	0.76%	2.37%
PIOB Rate Due to Initial Third Party Error	2.52%	6.51%
Total PIOB Rate	3.28%	8.88%

Table 3.6 illustrates the number of NSLs reviewed, the number of possible intelligence violations found in the 42 case files reviewed by the FBI and re-checked by the OIG, and the rate (occurrence of errors) at which the FBI and the OIG found possible intelligence violations within the sample reviewed.

TABLE 3.6
Comparison of Possible NSL-Related IOB Violations Identified by the FBI and the OIG at Three Field Offices

Field Office	NSLs Reviewed by FBI	PIOB Violations Identified by FBI	FBI PIOB Violation Rate	NSLs Re-Reviewed by OIG	PIOB Violations Identified by OIG	OIG PIOB Violation Rate
#1	210	5	**2.38%**	57	2	**3.51%**
#2	121	3	**2.48%**	56	3	**5.36%**
#3	65	5	**7.69%**	56	10	**17.86%**
Totals	**396**	**13**	**3.28%**	**169**	**15**	**8.88%**

Most of the possible intelligence violations identified by the OIG should have been identified by FBI inspectors if the inspectors compared the data provided by the NSL recipient with the data requested in the NSL and determined whether the data provided was relevant to the investigation. The violations were readily apparent to the OIG upon a review of the case files. For example, we identified instances in which the dates on the information provided by the NSL recipients did not match the dates requested on the NSLs.

The five most serious possible intelligence violations identified by the OIG that were missed by the FBI's inspectors were:

- The receipt of telephone toll billing records for the "family plan" (multiple telephone numbers) of individuals who were not relevant to an authorized investigation; these telephone toll billing records were not sequestered and were maintained in an FBI case file. They were not uploaded into FBI data systems.[75]
- The NSL requested data on a wrong telephone number due to an FBI typographical error in the area code; these telephone toll billing records were not sequestered and were maintained in an FBI case file. They were not uploaded into FBI data systems.
- The NSL recipient provided telephone toll billing records for 1 year earlier than the time period requested by the FBI.
- Two instances in which documents reflecting receipt of responsive records specifically incorporated Social Security Numbers and date of birth information on individuals who were not relevant to the underlying investigation; the error was compounded when these documents were electronically uploaded into the ACS system by the field office that served the NSL.[76]

---

[75] The records obtained from the provider showed that the individual who was relevant to an authorized investigation was associated with the telephone number for the last 21 days of the 7-month period requested by the NSL. The FBI received additional telephone records related to two previous subscribers of the telephone number identified in the NSL. There was no indication that either of the previous subscribers were subjects of, or relevant to, any FBI investigation. The records of one of the previous subscribers included toll billing records for the telephone number listed in the NSL as well as multiple "family plan" lines for a period of 2½ months within the 7-month period. During its review of the case file, the OIG identified these records for the two prior subscribers more than a year after the records were provided to the case agent.

[76] The case agent in the field office that issued the NSL had noted on the responsive records: "individual account records not relevant to this matter. New subscriber not related to subject. Don't upload."

The OIG's re-examination of case files in three FBI field offices demonstrated that the procedures implemented by the FBI for reviewing case files were not effective in ensuring that all NSL-related possible intelligence violations were identified. While the OIG is unable to calculate a revised NSL-related PIOB violation rate for all field offices, our determination that the FBI's possible intelligence violation totals are understated is also supported by additional data from the FBI's field review. Specifically, in the FBI's follow-up reviews of NSLs in 6 field offices in which FBI inspectors had initially identified only 1 possible intelligence violation during the field review, the FBI identified 83 additional NSL-related possible intelligence violations.

B. OIG Analysis

1. The OIG's Conclusions Regarding the Field and Headquarters Reviews

Despite the short period of time that the FBI devoted to planning and conducting its nationwide NSL field review, we believe the FBI used a reasonable methodology in conducting the review, committed significant resources to the effort, and made examination and analysis of the results a high priority. The FBI's 2007 field and Headquarters NSL reviews confirmed that the types of deficiencies identified by the OIG in our first NSL report occurred throughout the FBI from 2003 through 2006. Moreover, the FBI's 2007 reviews demonstrated that these deficiencies occurred in even greater numbers than the OIG found in our first NSL report.

However, we also concluded that the FBI's field review did not provide a fully reliable baseline from which to measure future improvement in compliance with NSL authorities. The OIG's re-examination of case files in three field offices that were included in the FBI's March 2007 field review demonstrated that the FBI's review missed a significant number of possible intelligence violations and therefore understated the percentage of possible violations. We believe this occurred because of:

- the short time period devoted to planning the review,
- the inspectors' lack of prior experience in conducting national security investigations or handling NSLs, and
- the Inspection Division's inability to conduct effective quality control during the review at the field offices due to time constraints it imposed on the review.

In addition, we believe the results of the FBI's field review likely understated the rate of possible intelligence violations because of the extent to which the FBI's inspectors were unable to locate information provided in

response to NSLs. The inspectors were unable to locate or properly analyze the responsive records (such as financial records, credit reports, or telephone toll billing records) for almost 15 percent of the FBI's sample of NSLs issued within the 2003 to 2006 review period.[77] Without finding or fully reviewing the responsive records, FBI inspectors could not determine whether an unauthorized collection had occurred.[78] Given that unauthorized collections represented the substantial majority (576 of 640, or 90 percent) of NSL-related possible intelligence violations identified during the FBI's field review, it is likely that more possible intelligence violations would have been identified if all the responsive data for the NSLs reviewed by the FBI inspectors had been located and reviewed.[79]

Also, we note the FBI's categorization of 557 of the 576 instances of unauthorized collections (97 percent) as third party errors rather than FBI errors.[80] While the initial mistakes may be attributable to NSL recipients who provided more information than was requested in the NSLs, the FBI compounded the errors by the manner in which it handled the information. Significantly, upon receiving unauthorized information from third parties, case agents did not consistently recognize that they had received unauthorized information or, if they did, they did not take appropriate steps to sequester the information and self-report the violations to the FBI OGC.[81]

---

[77] As noted previously, the FBI inspectors could not locate records in response to 532 NSLs, and 1,175 NSLs (including the 532) were not fully reviewed because the inspectors could not find all relevant documents (approval EC, NSL, and responsive records) or were unable to make determinations as to whether a possible intelligence violation had occurred.

[78] The FBI was able to identify only one instance of unauthorized collection without reviewing the NSL-responsive records.

[79] In light of the OIG's findings in our first NSL report that NSL-derived information could not consistently be located in the four field offices we visited, the FBI OGC issued guidance in January 2007 requiring that NSL-derived records be reviewed before uploading into FBI databases. This requirement was reiterated and expanded in the June 1, 2007, Comprehensive Guidance EC requiring that case agents ensure the NSL-derived information is responsive to the request and stored in the appropriate investigative file, and that receipt is documented. This and other recent NSL guidance are described in Chapter Two of this report.

[80] As shown in Table 3.2, FBI inspectors identified 676 third party errors (these matters are included in the 364 and 312 totals). However, in 117 instances, the same violation was reported in both third party error unauthorized collection totals and, in 2 additional instances, were also reported as FBI typographical errors. When the duplicate entries are removed, the balance is 557 violations due to initial third party errors.

[81] Guidance to the field issued by the FBI OGC on November 16, 2006, stated that if the field improperly or unintentionally acquires information through an NSL, the case agent should sequester the information with the CDC pending resolution of the potential intelligence violation by the FBI OGC. The FBI OGC thereafter advises the field whether the information may be used or whether the information must be returned to the carrier or be

(Cont'd.)

As noted above, of the 557 identified possible intelligence violations that resulted initially from third party errors, case agents self-reported only 4 (less than 1 percent).[82] We determined in our field office reviews that because the unauthorized information was not identified and sequestered, FBI agents incorporated the information into their case files. Additionally, in some cases, according to an FBI Inspection Division supervisor, this information was uploaded into the FBI's Telephone Applications database, which in turn is shared with other members of the Intelligence Community. Pursuant to the IOB's August 1, 2007, directive, the FBI OGC will be assessing whether the FBI compounded initial third party errors in the matters reported to it from the FBI's 2007 reviews.

The OIG also is concerned with the FBI's characterization of various infractions 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 NSL report, 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.[83] By calling these "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. We believe that proper supervisory and legal review of all NSL-related documents are required to ensure compliance with NSL statutes, the Attorney General's NSI Guidelines, as well as internal FBI policies. 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. These officials agreed to consider using a different label, such as "lapses in internal controls," to describe these types of deficiencies.

---

destroyed with appropriate documentation to the file. On November 30, 2006, the FBI OGC issued internal guidance stating that case agents are required to report to the FBI OGC the unauthorized collection of information obtained in response to NSLs, but that these matters are not reportable to the IOB. National Security Law Branch (NSLB), Federal Bureau of Investigation, memorandum to NSLB Attorneys, Guidance for Drafting IOB Opinions, November 30, 2006, 6-7. However, on August 1, 2007, the IOB directed the FBI to report instances in which the FBI "compounds a third party error by utilizing the inappropriately provided information or uploading the information into Bureau databases . . . ."

[82] The FBI's failure to self-report violations was not limited to unauthorized collections. Only 2 of the other 64 possible intelligence violations (640 minus 576) determined to be improper requests or improperly authorized NSLs had previously been reported to the FBI OGC through mandatory self-reporting.

[83] NSL I, 103-107.

2. The OIG's Conclusions Concerning the FBI's FCRA Review

In our first NSL report the OIG identified instances in which consumer 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 violation of the FCRAv NSL statute. The FBI responded by undertaking a comprehensive review of all such FCRA NSLs issued from January 1, 2002, through December 31, 2006, to determine whether these NSLs improperly requested 1681v consumer full credit reports or resulted in the receipt of unauthorized collections of consumer full credit reports in the absence of an international terrorism nexus. The review confirmed that such violations of the FCRA statutory requirements had occurred. For example, the FBI review identified 33 improper requests seeking consumer full credit reports and 233 unauthorized collections of these reports.

To put these violations of the FCRA in perspective, we calculated the number of violations identified in the FBI's 2007 FCRA review in relation to the total number of FCRA NSLs issued in counterintelligence investigations during the 2002 through 2006 review period:

- The 33 improper FCRAv requests represent an error rate of [redacted] percent since the FBI issued [redacted] FCRAv NSLs in counterintelligence investigations during the 5-year review period.[84]
- The 233 unauthorized collections obtained in response to FCRAu NSLs represent an error rate of [redacted] percent since the FBI issued [redacted] FCRAu NSLs in counterintelligence investigations during the review period.[85]

The results of the FBI's FCRA review demonstrate that confusion or lack of knowledge of the statutory requirements was present among case agents, supervisors, and CDCs throughout 2006. Consequently, the FBI's

---

[84] This calculation is based on data we analyzed from the FBI OGC's NSL tracking database.

[85] We compared the 13 possible FCRAv intelligence violations identified in the field review to the 33 possible FCRAv intelligence violations that the FBI identified in its 100-percent review of counterintelligence investigations between 2002 and 2006 in which FCRAv NSLs were issued without a nexus to international terrorism. We assumed that all 13 FCRAv matters would be among the 33 FCRAv identified in the 100-percent review. We had sufficient information to definitely match 11 of the 13. We could not match the other two matters. In one, the field office reporting in the 100-percent review did not include sufficient identifying information. In the other matter, the field review reported that a FCRAv NSL was issued but the responsive records could not be located.

mandatory self-reporting mechanism was not effective: only [redacted] of the [redacted] FCRA NSLs issued in counterintelligence investigations that were either improper requests or resulted in unauthorized collections – 3 percent – were self-reported to the FBI OGC.[86] It appears that case agents, their supervisors, the CDCs, and the Special Agents in Charge did not recognize that they made improper requests under the FCRA. Similarly, neither the case agents nor the analysts who reviewed records responsive to these NSLs recognized that they had received unauthorized information in response to FCRA NSLs. For the most part, FBI field offices offered no explanation for the results they reported to the FBI OGC.

III. OIG Conclusions and Recommendations

In conclusion, we found that the violations identified during the FBI's 2007 Headquarters and field reviews, as well as the OIG's 2006 and 2007 field reviews, demonstrate that the additional remedial measures being implemented by the FBI are necessary and should remain a priority. These measures are required to ensure that: (1) the FBI adheres to national security letter authorities, Attorney General Guidelines, and internal FBI policies; (2) supervisors and CDCs provide close and independent reviews of NSLs; and (3) possible intelligence violations arising from the use of NSL authorities are promptly identified and accurately reported to the FBI OGC and, when required, to the IOB. Based on the results of the FBI's FCRA NSL review and other information about FCRA NSLs discussed elsewhere in this report, and the high percentage of instances in which the NSL-derived information could not be located by FBI and OIG inspectors, we believe the FBI must continue to reinforce the distinctions among the FBI's FCRA NSL authorities and ensure that any improperly obtained information is identified, sequestered, and reported as appropriate, and develop guidelines to improve the ability to locate NSL-derived information.

We therefore recommend that the FBI:

1. Reinforce the distinction between the FBI's NSL authorities pursuant to the *Fair Credit Reporting Act* (FCRA) throughout all levels of 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 Assistant Special Agents in Charge and Special Agents in Charge.

---

[86] The 266 total is composed of 33 improper requests plus 233 unauthorized collections.

2. Add procedures to include reviews of FCRA NSLs issued in counterintelligence investigations in the FBI Inspection Division's periodic reviews and in the National Security Division's national security reviews (described in Chapter Two of this report).

3. Reiterate in its 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.

4. 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.

5. Issue additional guidance addressing the filing and retention of NSL-derived information that will improve the ability to locate NSL-derived information. The guidance should require that all NSL-derived information be appropriately documented, stored, easily identified, and readily available for internal and external review.

6. Include in its routine case file reviews and the National Security Division's national security reviews an analysis of the FBI's compliance with requirements governing the filing and retention of NSL-derived information.

CHAPTER FOUR:
NATIONAL SECURITY LETTER REQUESTS ISSUED BY THE FBI IN 2006

In this chapter, we describe the FBI's data on the use of national security letters during calendar year 2006. However, for reasons discussed in our previous report on NSLs, we believe that the data provided by the FBI from the Department's semiannual classified reports to Congress and the FBI Office of the General Counsel (FBI OGC) national security letter tracking database (OGC database) do not accurately reflect the total number of NSL requests issued in 2006.

In our first NSL report we documented various technical and structural problems with the OGC database that resulted in inaccuracies and a significant understatement of NSL requests in the Department's reports to Congress. While noting the limitations of the OGC database, we provided in our first NSL report a summary and analysis of data derived in large part from the database because that database was the only centralized repository of data reflecting the FBI's use of national security letter authorities.

Moreover, in our investigation of the FBI's use of exigent letters, which will be described in our forthcoming NSL report, we found additional inaccuracies in the Department's semiannual classified reports to Congress and the OGC database. We determined that the FBI sought or obtained records or other information on thousands of telephone numbers outside the normal approval process, some of which were associated with improper NSLs, exigent letters, or other informal requests. Among these non-routine NSLs were 11 "blanket" NSLs that sought telephone data on approximately 3,860 telephone numbers (8 percent of all NSL requests captured by the OGC database in 2006). These NSLs were issued in an attempt to validate the FBI's earlier acquisition of data from three communication service providers pursuant to contracts with the FBI. The requests contained in these NSLs were not uploaded into the OGC database because they were not documented by electronic communications (EC) with leads sent to FBI OGC for purposes of compiling data for congressional reporting. The FBI told us that, after eliminating duplicates, there were 2,196 unique telephone numbers in the 11 blanket NSLs.

Our forthcoming NSL report will describe in more detail the circumstances surrounding issuance of these NSLs, including the fact that the FBI did not generate approval ECs before these NSLs were signed by senior FBI officials; some of the NSLs were signed by FBI personnel who were not authorized to sign NSLs; and some NSLs did not comply with the Patriot Reauthorization Act requirements regarding non-disclosure provisions.

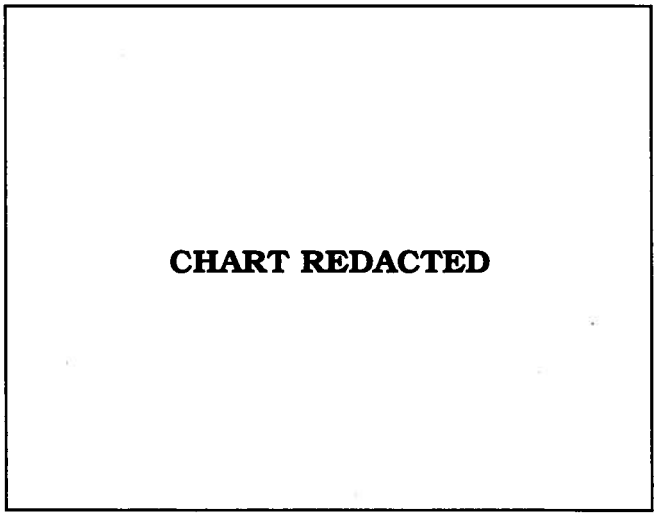
With these caveats, we discuss in the balance of this chapter the data on NSL usage that was contained in the OGC database and in the 2006 semiannual classified reports to Congress. In Section I we discuss the methodology we used to collect and analyze the FBI data on NSL use in 2006. In Section II we report on the number of NSL requests issued in 2006. In Section III we present data on overall trends in the FBI's NSL usage from 2003 through 2006.

I. Methodology

For this review, the OIG analyzed data in the FBI OGC database related to NSLs issued during calendar year 2006.[87] The FBI used this database to collect the data it needed to prepare the Department's annual public reports and semiannual classified reports to Congress on NSL usage. We also examined these annual public reports to evaluate NSL requests in 2006 and to analyze trends in NSL usage from 2003 through 2006.

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. In our analysis, we refer to the number of national security letter requests rather than the number of national security letters because one NSL may include more than one request. For example, one NSL to a telephone company may request information on many telephone numbers. The data presented in the Department's semiannual classified reports to Congress and in its annual public reports are the numbers of requests made, not the number of letters issued. In this

CHART 4.1
Relationship between Investigations, NSLs, and NSL Requests in 2006



Source: FBI OGC database as of May 2007

[87] After we completed our analysis of the FBI OGC NSL database, the FBI provided the OIG with an updated database in January 2008 that included a small amount of additional data for the third and fourth quarters of the semiannual classified reports to Congress for 2006. The January 2008 version of the database included [redacted] (0.5 percent) more NSLs and [redacted] (4 percent) more NSL requests than the May 2007 database that we used for our analyses. We determined that this small amount of additional NSLs and NSL requests would not materially change our analyses.

report, we follow that same approach. Chart 4.1 shows the relationship between the numbers of investigations, NSLs, and NSL requests in 2006.

We used the OGC database for this information because it was the only centralized source on the Department's use of NSLs during 2006. As noted above, our first NSL report documented flaws in the internal reporting of NSLs and structural problems with the OGC database that affected the accuracy and reliability of the Department's semiannual classified reports to Congress.[88] Since the OIG issued its first NSL report, the FBI has taken steps to upgrade the technology it uses to generate NSLs and related documents.[89]

The Department was required to file semiannual classified reports to Congress describing the total number of NSL requests issued pursuant to four of the five NSL authorities: *Right to Financial Privacy Act* (financial records), *Electronic Communications Privacy Act* (telephone toll billing records, electronic communication transactional records and subscriber information (telephone or e-mail)), and two *Fair Credit Reporting Act* authorities (for consumer and financial institution-identifying information and consumer full credit reports).[90] In addition, beginning in March 2006 pursuant to amendments to the NSL authorities in the Patriot Reauthorization Act, the Department was required to provide annual public reports on certain aspects of its NSL usage.

In its classified reports, the Department described:

(1) the number of investigations of different persons or organizations that generated NSL requests and

(2) the number of requests made in those investigations.

---

[88] See NSL I, 31-36.

[89] In Chapter Two of this report, we provide a description and our analysis of the FBI's efforts to improve the accuracy of the OGC database and the public and classified reports to Congress that are generated using this data.

[90] Prior to the Patriot Reauthorization Act, the Department was required to provide reports to Congress only on its use of its NSL authorities under the *Right to Financial Privacy Act* (RFPA), the *Electronic Communications Privacy Act* (ECPA), and under the *Fair Credit Reporting Act* (FCRA) for consumer and financial institution-identifying information. The Patriot Reauthorization Act requires the Department also to report on use of its NSL authority pursuant to the FCRA for consumer full credit reports. See § 118(b) of the Patriot Reauthorization Act. The Department is not required to report the number of NSL requests issued pursuant to the *National Security Act* NSL statutes (authorizing the FBI to obtain financial records, other financial information, and consumer reports).

Based on data uploaded into the OGC database and the semiannual classified reports to Congress, we separated these totals into different categories for investigations of "U.S. persons or organizations" and "non-U.S. persons or organizations."[91]

II. National Security Letter Requests Issued in 2006

In this section, we describe the FBI's use of NSLs in 2006 as documented in the OGC database. We describe the total number of NSL requests as well as NSL requests relating to investigations of U.S. persons and non-U.S. persons. We also include a breakdown of the proportion of NSL requests issued during counterterrorism, counterintelligence, and foreign computer intrusion cyber investigations.

In 2006, the FBI issued a total of 48,106 NSL requests pursuant to four of the five national security letter authorities.[92] As shown in Chart 4.2, the overwhelming majority of these requests sought telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the *Electronic Communications Privacy Act* (ECPA) NSL statute.[93] The second most frequently used NSL authority, accounting for approximately [redacted] percent of the total, sought records from financial institutions, such as banks, credit card companies, and finance companies under the *Right to Financial Privacy Act* (RFPA) authority. These records include open and closed checking and savings accounts. The remaining [redacted] percent of the NSL requests were issued pursuant to the two *Fair Credit Reporting Act* (FCRA) NSL authorities and sought either financial institution- or consumer-identifying information or consumer full credit reports.[94]

---

[91] 50 U.S.C. § 1801(i) defines a "United States Person" as:

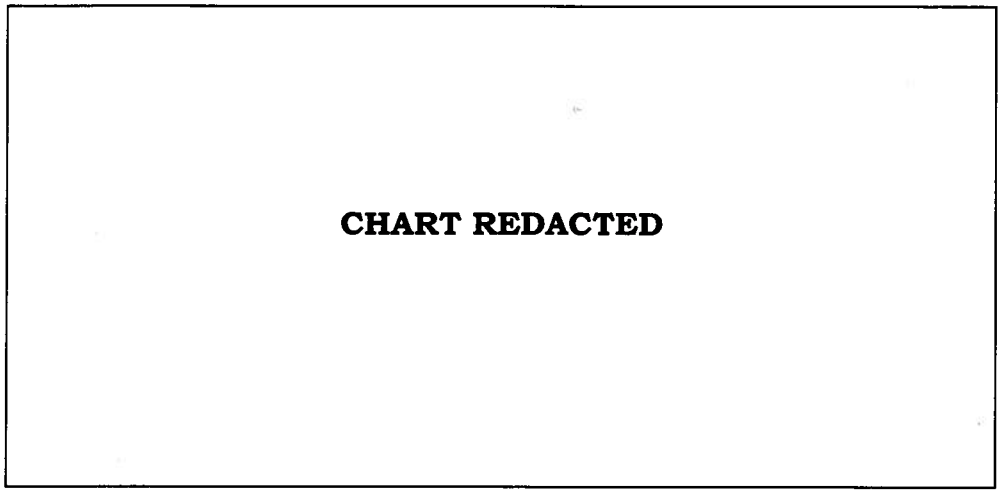
> a citizen of the United States, an alien lawfully admitted for permanent residence . . ., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United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

[92] FBI records show that [redacted] national security letters were issued pursuant to the *National Security Act* NSL statute in 2006.

[93] Electronic communication transactional records (e-mails) may include e-mail addresses associated with the account, screen names, and billing records and method of payment for the account.

[94] A detailed description of the number of NSL requests for each of the four types of NSLs in counterterrorism and counterintelligence investigations is included in the Classified Appendix to this report.

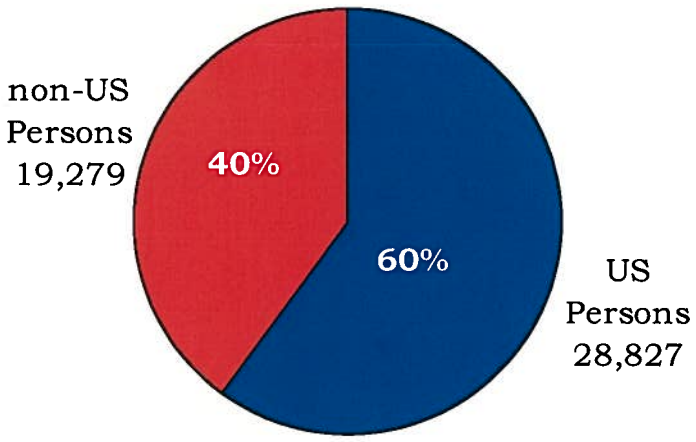
CHART 4.2
NSL Requests (2006)



Source: FBI OGC NSL database as of May 2007

As shown in Chart 4.3, the majority of NSL requests issued in 2006 were generated from investigations of U.S. persons.

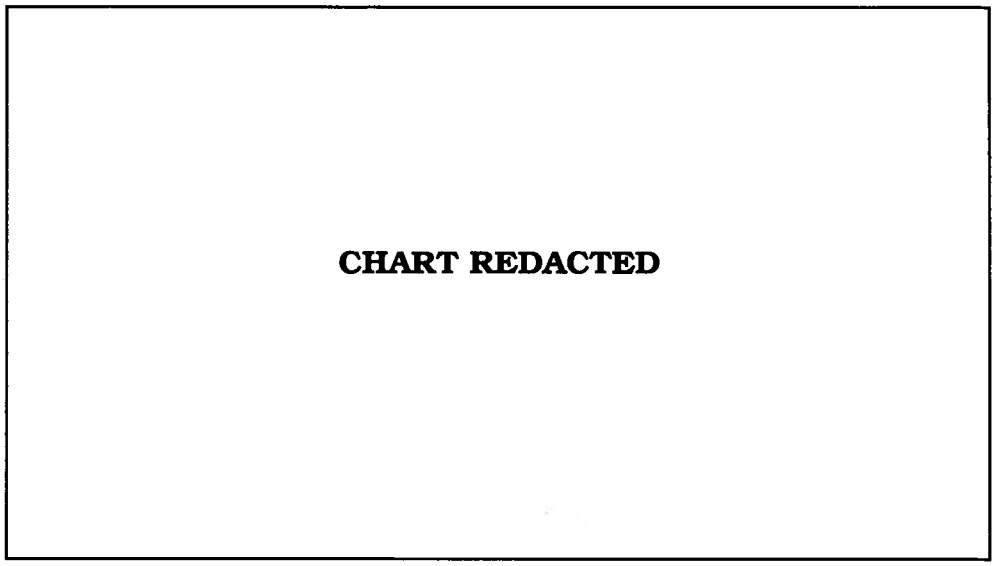
CHART 4.3
NSL Requests Relating to Investigations of U.S. Persons and non-U.S. Persons (2006)



Source: FBI OGC NSL database as of May 2007

FBI data showed that in 2006 approximately [redacted] percent of all NSL requests were issued during counterterrorism investigations, approximately [redacted] percent were issued in counterintelligence investigations, and approximately [redacted] percent were issued in foreign computer intrusion cyber investigations (Chart 4.4).

CHART 4.4
NSL Requests in Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations (2006)



Source: FBI OGC NSL database as of May 2007

FBI data showed that on average approximately one third of all counterterrorism, counterintelligence, and cyber investigations that were open at any time during 2006 used NSLs. NSLs were used in [redacted] counterintelligence investigations ([redacted] percent) than in counterterrorism investigations ([redacted] percent) or cyber investigations ([redacted] percent) in 2006, as shown in more detail in the Classified Appendix to this report.

III. Trends in National Security Letter Usage from 2003 through 2006

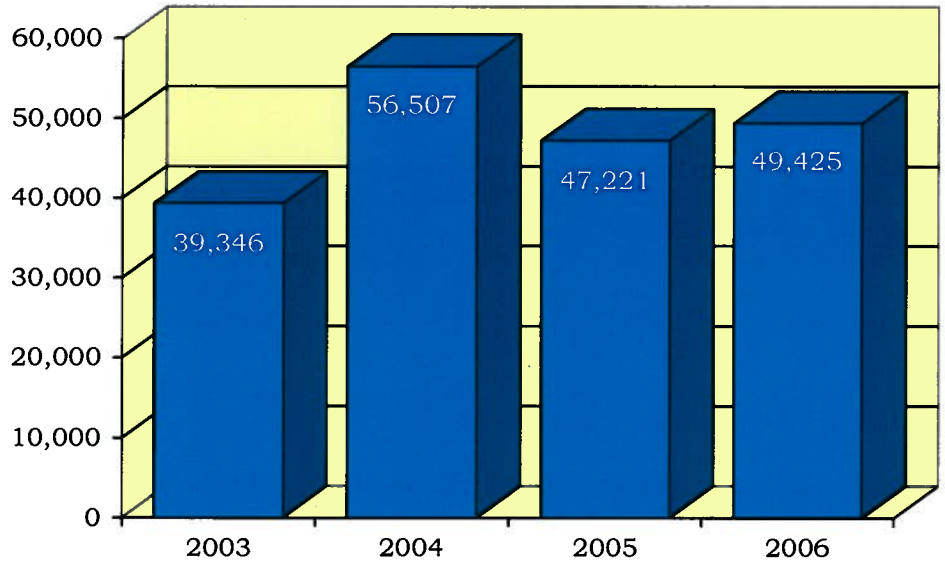
In this section, we describe the general levels and trends in the FBI's NSL requests from 2003 through 2006 as documented in the Department's semiannual classified reports to Congress and the OGC database, when applicable.

According to the Department's semiannual classified reports to Congress from 2003 through 2006 and information in the OGC database, the FBI issued a total of 192,499 NSL requests pursuant to its RFPA, ECPA, and FCRA NSL authorities during this 4-year period.[95] The total number of NSL requests issued by the FBI rose slightly (approximately 5 percent) in

[95] As we reported in our first NSL report, this total includes [redacted] NSL requests for consumer full credit reports issued from 2003 through 2005 that the Department was not required to include in its reports to Congress. See NSL I, 36.

2006 over the 2005 levels. Chart 4.5 illustrates the total number of NSL requests issued during each of the years from 2003 through 2006.

CHART 4.5
NSL Requests (2003 through 2006)



Sources: DOJ semiannual classified reports to Congress and FBI OGC database as of May 2006 (for 15 U.S.C. § 1681v NSL requests in 2003 through 2005)

FBI data showed that from 2003 through 2006, the overwhelming majority (about [redacted] percent) of the FBI's NSL requests sought telephone toll billing records information, subscriber information (telephone or e-mail), or electronic communication transactional records under the ECPA NSL statute. The second most frequently used type of NSL request, accounting for approximately [redacted] percent of the total, sought financial records (for example, open and closed checking and savings accounts) from financial institutions such as banks, credit card companies, and finance companies under the RFPA authority. The remaining [redacted] percent of the NSL requests were issued pursuant to the two FCRA NSL authorities and sought either financial institution- or consumer-identifying information or consumer full credit reports.[96]

NSL Requests Relating to U.S. Persons and non-U.S. Persons: FBI data also showed that the percentage of NSL requests generated from investigations of U.S. persons versus non-U.S. persons shifted over the

[96] We provide a more detailed analysis of trends in the FBI's use of each of the four types of NSLs over the 4-year period in the Classified Appendix to this report.

4-year period. In 2003, approximately 39 percent of NSL requests were generated in the course of investigations of U.S. persons. However, the number of NSL requests generated from investigations of U.S. persons almost doubled from 6,519 in 2003 to 11,517 in 2006, which represented 57 percent of all NSL requests in that year. During the same period, the number of NSL requests generated from investigations of non-U.S. persons declined from 10,232 in 2003 to 8,605 in 2006.

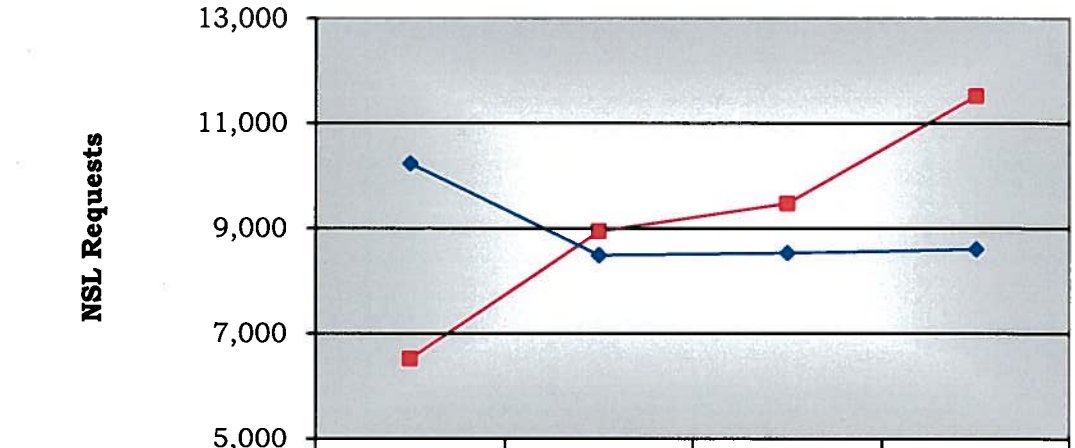
The Executive Assistant Director of the FBI's National Security Branch (NSB) provided several reasons for the increase in NSLs involving U.S. persons over the 4-year period. He stated that as the FBI has moved forward from the investigations of the September 11 attacks, it has focused on investigations of possible sleeper cells in the United States and conducted follow-up investigations of terrorist activities in the United Kingdom and elsewhere to determine if there is a U.S. nexus to those events. He also pointed to the FBI's interactions with state and local law enforcement agents, the work of the FBI's Field Intelligence Groups, and the investigations conducted by Joint Terrorism Task Forces, all of which have generated leads involving U.S. persons that result in the initiation of national security investigations and the issuance of NSLs.

Chart 4.6 depicts the number of NSL requests generated from investigations of U.S. persons and non-U.S. persons from 2003 through 2006.[97]

---

[97] Chart 4.6 does not contain the same totals as Chart 4.5 because the FBI is not required to report the U.S. person status of targets of subscriber NSLs. Specifically, 117,111 NSL requests seeking subscriber information for telephone numbers and Internet e-mail accounts in 2003 through 2006 did not identify the subject's status as a U.S. person or non-U.S. person. Similarly, while the FBI captured data on the status of persons who were the targets of consumer full credit reports issued in 2003 through 2005, the Department was not required to include this data in its reports. Beginning in 2006, the Patriot Reauthorization Act required the Department to report to Congress the status of targets of its NSL requests for consumer full credit reports. Thus, we do not include in Chart 4.6 the [redacted] NSL requests that the OGC database identified as having been issued in 2003 through 2005 and the [redacted] NSL requests reported to Congress in 2006 for consumer full credit reports pursuant to 15 U.S.C. § 1681v.

CHART 4.6
NSL Requests Relating to U.S. Persons and non-U.S. Persons (2003 through 2006)



	2003	2004	2005	2006
Non-U.S. Persons	10,232	8,494	8,536	8,605
U.S. Persons	6,519	8,943	9,475	11,517

Source: DOJ semiannual classified reports to Congress

NSL Requests Issued During Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations: Chart 4.7 shows the distribution of NSL requests issued from the three types of investigations during the 4-year period. Overall, NSL requests issued in counterterrorism investigations accounted for a substantial majority of all requests. The proportion of NSL requests issued in counterintelligence investigations was [redacted] in 2004 ([redacted] percent) than in 2003, 2005, and 2006 (ranging from [redacted] percent in 2003 to [redacted] percent in 2006).[98] The data also showed that the proportion of NSL requests issued in foreign computer intrusion cyber investigations was [redacted] in 2006 ([redacted] percent) than in previous years ([redacted] percent).

[98] In 2004, the FBI issued 9 NSLs seeking subscriber information on 11,100 telephone numbers in connection with a single investigation.

CHART 4.7
NSL Requests in Counterterrorism, Counterintelligence, and Foreign Computer Intrusion Cyber Investigations (2003 through 2006)

CHARTS
REDACTED

Source: FBI OGC NSL database as of May 2006 and May 2007

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

In our first NSL report we examined the effectiveness of national security letters in different types of national security investigations conducted between 2003 and 2005. Based on our interviews of Headquarters and field personnel and our examination of case files in four FBI field offices, we described the value of each type of NSL as well as the analyses developed from NSLs that enable the FBI to identify communication and financial links between subjects of its investigations and others.[99]

Our first NSL report also described the principal uses of NSLs: to develop evidence to support applications for Foreign Intelligence Surveillance Act 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 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.

In this review, our examination of case files and interviews of FBI Headquarters officials and personnel in three FBI field offices confirmed that NSLs continued to be important tools in the FBI's national security investigations conducted in 2006. Many FBI personnel told us that NSLs are an essential and indispensable intelligence tool.

---

[99] See NSL I, 45-65.

FBI personnel provided the following examples of the value of NSLs issued pursuant to the *Right to Financial Privacy Act* (RFPA), the *Fair Credit Reporting Act* (FCRA), and the *Electronic Communications Privacy Act* (ECPA) in advancing national security investigations they conducted in 2006:

- A field office reported that information from national security letters enabled case agents to identify pertinent e-mail addresses, telephone numbers, and bank accounts that were used to support a subject's terrorist activities. The investigators used information derived from the ECPA and RFPA NSLs to identify the extent of a subject's circle of associates and his financial network. Case agents stated that information on the subject's financial network was essential in developing the money laundering portion of the case.
- In 2006, while investigating a plot to conduct terrorist activities, a field office served ECPA and RFPA NSLs to obtain financial, telephone subscriber, and telephone toll records for the subjects and their associates. Using this information, investigators identified the financial associates of several of the investigation's subjects while ruling out the possibility that a larger terrorist organization was financing the plot.
- A field office opened a counterterrorism investigation in the spring of 2006 and issued numerous ECPA and RFPA NSLs to communications providers and financial institutions. These NSLs assisted the investigators in confirming the identities of the subjects and were used in support of an application for authority to use additional investigative techniques. NSLs also identified financial institutions that the subjects used, which in turn led to the discovery of certain purchases.
- In the summer of 2005, the FBI received information suggesting that individuals associated with two e-mail addresses were in contact with known extremists. The FBI issued ECPA NSLs to two Internet service providers (ISP) associated with these e-mail addresses to determine the identity of the users. This information was insufficient to positively identify the users of the e-mail accounts. However, information received indicated that the majority of log-ins for both e-mail accounts could be traced to two different ISPs. The FBI served ECPA NSLs on these ISPs. Responsive records enabled the FBI to determine where the users of the e-mail addresses were located.
- In June 2006, the U.S. military [redacted]

[redacted] Because of the potential threat, the FBI initiated preliminary investigations on the U.S.-based subscribers of two telephone numbers and issued ECPA NSLs to identify the subscribers. The investigation is continuing.

- Two individuals in possession of weapons were stopped by law enforcement officials and an FBI national security investigation was initiated. Over the next few months a source reported that one of the subjects was planning to travel abroad to engage in armed jihad against U.S. and Coalition troops. A number of RFPA and ECPA NSLs were issued seeking financial information, credit reports, toll records, and e-mail account information on the primary subjects in this group.
- The FBI is investigating the foreign intelligence activities of a subject involved with a foreign government. An NSL has been served to assist the FBI in investigating a network for procuring illicit dual-use technology for use in a weapons of mass destruction program.
- In an FBI national security investigation, the FBI has issued NSLs that have helped to identify two FBI assets who were in contact with the subject of the investigation – contacts previously unknown to the FBI. The NSLs identified the subject's e-mail accounts, which in turn led to the issuance of additional NSLs. FBI counterintelligence personnel said that the imposition of the non-disclosure provisions in the NSLs has been critical in keeping the FBI's interest in the subject from coming to the attention of the foreign government involved in the matter.

CHAPTER SIX:
OIG FINDINGS ON THE FBI'S COMPLIANCE WITH THE PATRIOT REAUTHORIZATION ACT'S NON-DISCLOSURE AND CONFIDENTIALITY PROVISIONS

Section 119(b)(3)(E) of the Patriot Reauthorization Act directed the OIG to perform an audit of national security letters issued after the Act became effective in March 2006 to determine the number of occasions in which NSLs were issued "without the certification necessary to require the recipient of such letter to comply with the nondisclosure and confidentiality requirements potentially applicable under law."

In Section I of this chapter we describe the new certification requirement in the Patriot Reauthorization Act, the steps taken by the FBI to implement the new measures, and the methodology of the OIG's audit of the FBI's compliance with the certification requirements. Section II provides our findings and analysis, and Section III contains our conclusions and recommendation.

I. Background

A. The Patriot Reauthorization Act

As initially drafted, the NSL statutes imposed non-disclosure and confidentiality obligations on all NSL recipients.[100] The national security letter provisions of the *Right to Financial Privacy Act* (RFPA), *Electronic Communications Privacy Act* (ECPA), and the *Fair Credit Reporting Act* (FCRA) authorized the FBI to advise recipients that they were prohibited by statute from disclosing to anyone that the FBI had sought or obtained access to the requested records.[101]

The non-disclosure and confidentiality provisions of the three NSL statutes provoked significant public controversy and generated the first

---

[100] Throughout the national security letter statutes and Sections 116 and 117 of the Patriot Reauthorization Act, the terms "non-disclosure" and "confidentiality" are used interchangeably.

[101] Prior to the Patriot Act, the ECPA and the RFPA provided that no wire or electronic communication service provider or financial institution "shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records." 18 U.S.C. § 2709(c)(2000); 12 U.S.C. § 3414(a)(3)(2000). The FCRA authorized disclosure only to "those officers, employees, or agents of a consumer reporting agency necessary to fulfill the requirement to disclose information to the Federal Bureau of Investigation . . . ." 15 U.S.C. § 1681u(d)(2000).

judicial challenge to any of the Patriot Act amendments to the NSL statutes. See *Doe* v. *Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated by Doe* v. *Gonzales*, 449 F.3d 415 (2d Cir. 2006) *Doe* v. *Gonzales*, 386 F. Supp. 2d 669 (D. Conn. 2005), *dismissed as moot, Doe* v. *Gonzales*, 449 F.3d 415 (2d Cir. 2006), upon remand *Doe* v. *Gonzales*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007) (holding non-disclosure provision in the Patriot Reauthorization Act, 18 U.S.C. § 2709, to be unconstitutional under the First Amendment).

The Patriot Reauthorization Act modified the non-disclosure and confidentiality obligations on NSL recipients. The Act authorized the FBI to impose these obligations only upon certification of specified harm that might arise in the underlying investigation if a disclosure occurred. Specifically, after March 9, 2006, if the FBI seeks to impose non-disclosure and confidentiality disclosure requirements on an NSL recipient, the Patriot Reauthorization Act requires the FBI Director or his designee to certify that disclosure of the FBI's demand for information might result in:

- danger to the national security of the United States;
- interference with criminal, counterterrorism, or counterintelligence investigations;
- interference with diplomatic relations; or
- danger to the life or physical safety of any person.[102]

If the certifying official determines that confidentiality is necessary, Section 116 of the Patriot Reauthorization Act requires that recipients be notified of three specific obligations:

(1) that receipt of the NSL must remain confidential and cannot be disclosed except as required to comply with the NSL or to obtain legal advice from an attorney;

(2) if the recipients disclose 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.[103]

---

[102] Patriot Reauthorization Act, § 116 (2006). The Act provides that the Director's designee must not be in a position lower than a Headquarters Deputy Assistant Director or field division Special Agent in Charge designated by the Director. Id.

B. The FBI's Implementation of the Patriot Reauthorization Act Non-Disclosure and Confidentiality Requirements

On March 9, 2006, the date the President signed the Patriot Reauthorization Act, the FBI OGC notified all Special Agents in Charge (SAC) and Chief Division Counsels (CDC) that the NSL models that had been posted on FBI OGC's National Security Law Branch (NSLB) Intranet website could no longer be used to generate NSLs. The FBI OGC advised FBI personnel that all NSLs that had been prepared but not yet served would have to be redrafted to conform to the new requirement in the law.

To implement the new law, on March 9, 2006, the FBI Director delegated certification authority to all SACs and other designated senior officials.[104] In the delegation memorandum, the FBI OGC advised that non-disclosure certifications "should not and may not be made in a perfunctory manner." The delegation also stated that the individual signing the NSL must make an assessment that there is "a genuine need for non-disclosure" based on one of the possible dangers listed in the statute that could result from disclosure.[105]

The FBI OGC concurrently disseminated guidance on the provisions of the new law to FBI Headquarters and field divisions. Also on March 9, the FBI OGC distributed revised NSL approval ECs and NSL models to all SACs and CDCs and posted the new models on the FBI OGC's Intranet website.[106] The FBI OGC advised that the non-disclosure provision could no

---

[103] NSL recipients are not required to divulge to the FBI that they intend to consult an attorney to obtain legal advice or legal assistance about the NSL. Patriot Reauthorization Act, § 116 (2006).

[104] In addition to the SACs, the Director delegated certification signature authority, non-disclosure certification authority, and non-disclosure recertification authority for NSLs to the following FBI senior officials: Deputy Director; Executive Assistant Director and Assistant Executive Assistant Director for the National Security Branch; Assistant Directors and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; General Counsel and Deputy General Counsel for the National Security Law Branch; and Assistant Directors in Charge of the New York, Washington, D.C., and Los Angeles field offices.

[105] Office of the General Counsel, Federal Bureau of Investigation, electronic communication to all Divisions, Delegation of Non-Disclosure Certification Authority, March 9, 2006, at 4.

[106] FBI policy requires that all NSLs and approval ECs contain certain information. NSL approval ECs must provide "predication" for the NSL by explaining why the information sought is relevant to an authorized investigation; document approval of the NSL by appropriate personnel; certify the necessity for non-disclosure and confidentiality when applicable; include information needed to fulfill congressional reporting requirements; and document transmittal information for the NSLB, the responsible Headquarters division, and the division that is asked to serve the NSL. The NSL must identify the statutory authority for the request and types of records requested; contain identifying information for (Cont'd.)

longer automatically be included in NSLs and explained the certification process. The FBI OGC repeatedly emphasized through e-mails to all CDCs, communications with individual CDCs, and the new models it generated that certifications for imposing the non-disclosure obligation were not to be perfunctory or automatic.

On March 15, 2006, the FBI OGC issued further guidance reiterating that the non-disclosure provision was "no longer automatically included in the NSL" and that the FBI must ensure that there is a "genuine need" for non-disclosure prior to use. To amplify the statutory directive noted above, the FBI OGC guidance explained that when the non-disclosure provision is sought, the approval EC must provide a factual predicate to justify imposition of the provision.[107] The guidance listed the 4 potential harms noted in the Act (quoted above) and suggested the following 13 adverse consequences that case agents should consider in articulating the factual predicate justifying non-disclosure:

1. Disclosure may [redacted].
2. Disclosure may [redacted].
3. Disclosure may [redacted].
4. Disclosure may [redacted].

---

the targeted individual or account; certify that the records are relevant to an authorized investigation; certify, when applicable, that disclosure may result in an adverse consequence; and provide the notifications listed above to the recipient. For a more detailed description of these requirements, see NSL I, 22-27.

[107] According to the NSLB Intranet website, "[if] a non-disclosure provision is sought, the EC must set forth a factual predicate to require such a provision."

5. Disclosure may [redacted].

6. Disclosure may [redacted].

7. Disclosure may [redacted].

8. Disclosure may [redacted].

9. Disclosure may [redacted].

10. Disclosure may [redacted].

11. Disclosure may [redacted].

12. Disclosure may [redacted].

13. Disclosure may [redacted].

The FBI OGC also advised case agents to identify in their approval ECs any other reasons for imposing non-disclosure and confidentiality requirements if they were not on the list.

C. Methodology of the OIG Review

1. Random Sample of NSLs Issued After March 9, 2006

To perform our audit of the FBI's compliance with the non-disclosure and confidentiality provisions of the Patriot Reauthorization Act, we identified a statistically valid random sample of all NSLs issued from March 10, 2006, through December 31, 2006. By reviewing those NSLs to determine the number of NSLs that imposed non-disclosure and

confidentiality obligations, we could project how many NSLs issued throughout the FBI during that period imposed these conditions.

The FBI provided us with the FBI OGC NSL tracking database for calendar year 2006, which we used to determine the universe of national security letters issued during the relevant time period. The database contained 15,187 records, each representing one national security letter issued from March 10, 2006, through December 31, 2006. We determined that a sample size of 375 NSLs would permit us to project from the sample to the universe of all NSLs issued from March 10, 2006, through December 31, 2006, at a 95 percent confidence level. We then sequentially numbered the 15,187 records and used a random number generator to produce a list of 500 numbers (to ensure an adequate list of NSLs if the FBI was unable to produce every NSL we requested). We used the first 375 random numbers to locate the corresponding NSL in the OGC database, and we obtained copies of the NSLs and corresponding approval ECs.[108]

Our random sample included NSLs from 51 different FBI field offices and Headquarters divisions. The number of NSLs from each office ranged from 1 to 37.[109] Counterterrorism investigations generated 243 of the 375 NSLs in the sample, counterintelligence investigations generated 127 NSLs, and foreign computer intrusion cyber investigations generated 5 NSLs.[110]

---

[108] As we noted in our first NSL report, during the period 2003 through 2005 the FBI did not require case agents or others to retain copies of signed NSLs. As described in Chapter Three of this report, the directive to retain signed copies of NSLs was issued in March 2007 in conformity with one of our recommendations in our first NSL report. Accordingly, to perform this audit we had to use unsigned copies of NSLs that we obtained from a query of the FBI Automated Case Support (ACS) system.

For a variety of reasons, the FBI was unable to provide 56 NSL approval ECs and corresponding NSLs from our original list in response to our request. These reasons included instances in which NSLs were not electronically uploaded into the FBI ACS system, the requested documents were subject to access restrictions or had been permanently "charged out" or removed from the database, or the case file or serial numbers did not exist. When this occurred, we requested replacement records based on the random numbers we had generated.

[109] Three NSLs in our random sample were issued from FBI Headquarters case files.

[110] The distribution of NSLs among the counterterrorism, counterintelligence, and cyber investigative programs in our random sample was [redacted] to the distribution recorded in the FBI NSL tracking database for NSLs issued throughout 2006, an issue we address in Chapter Four of this report. Our analysis of the OGC database found that [redacted] of all NSLs issued during calendar year 2006 were generated from counterterrorism investigations, [redacted] from counterintelligence investigations, and [redacted] from cyber investigations. This is [redacted] to the distribution we found in our random sample: [redacted] generated from counterterrorism investigations, (Cont'd.)

For purposes of evaluating compliance with applicable non-disclosure and confidentiality requirements in the Act and other FBI policies, we reviewed both the NSL approval ECs and the NSLs. We examined the approval ECs to determine whether they:

- identified a national security investigation or foreign computer intrusion cyber investigation file number; and
- contained either a certification that disclosure that the FBI sought the requested information would result in the adverse consequences listed in the statute or a determination that the case did not warrant activation of the non-disclosure provision.[111]

We then determined whether the approval EC included a justification for non-disclosure and confidentiality. If a justification was included, we next determined whether that justification referenced any of the 13 possible adverse consequences listed on the FBI OGC Intranet website or identified other adverse consequences. We also examined the NSLs to determine whether they included non-disclosure and confidentiality obligations.

2. Other 2006 NSLs Identified During the Review

In addition to our analysis of the random sample of 375 NSLs, we identified 8 "blanket" NSLs issued after March 9, 2006, that we found did not comply with the Patriot Reauthorization Act non-disclosure and confidentiality requirements. We identified these blanket NSLs in our investigation of the FBI's use of exigent letters. In that investigation, we learned that the FBI's Counterterrorism Division issued at least 11 follow-up blanket NSLs to "cover" information obtained by personnel in the FBI's Communications Analysis Unit at FBI Headquarters in response to exigent letters or other informal requests. These NSLs sought telephone toll billing records for 3,860 telephone numbers (which corresponded to approximately 2,196 unique telephone numbers) pursuant to the ECPA NSL statute. None of these NSLs was accompanied by approval ECs, a violation of FBI policy. As a result, we were unable to determine whether the senior FBI officials

---

[redacted] from counterintelligence investigations, and [redacted] from cyber investigations.

[111] The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection require that NSLs be issued only in connection with national security investigations. FBI policy requires that NSLs be issued from investigative files, not from control files. See NSL I, 100-104. We reviewed the approval ECs accompanying the 375 NSLs to determine whether they complied with this requirement. Of the 375 approval ECs we examined, we found 1 instance in which an approval EC indicated that the FBI relied exclusively on an FBI Headquarters control file rather than an investigative file to initiate approval for the issuance of an NSL.

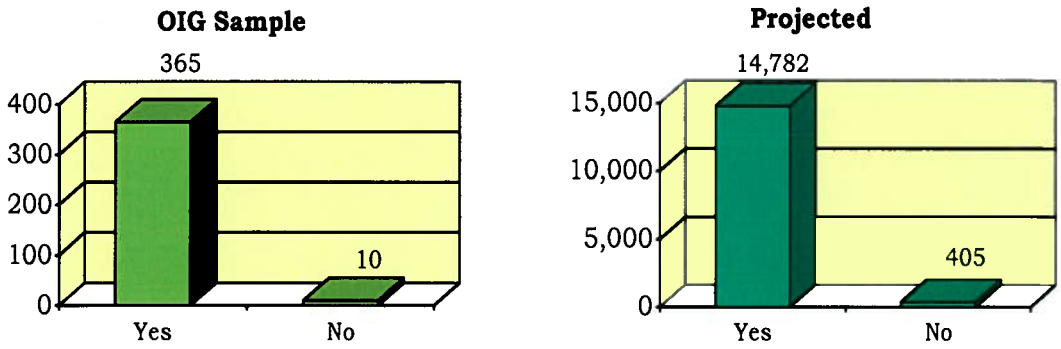
who signed these NSLs considered whether there was adequate predication to impose the non-disclosure and confidentiality obligations that were referenced in 8 of the 11 NSLs. We will provide more details and our analysis of these NSLs in our forthcoming NSL report.

II. OIG Findings and Analysis

A. NSLs That Invoked Non-Disclosure and Confidentiality Obligations

Of the 375 NSLs we examined in our random sample, 365, or 97 percent imposed the non-disclosure and confidentiality obligation established in the Patriot Reauthorization Act. Based on that result, we projected that of the 15,187 NSLs the FBI issued from March 10, 2006, through December 31, 2006, 14,782 NSLs imposed the non-disclosure and confidentiality obligations.

CHART 6.1
NSLs that Imposed Non-Disclosure and Confidentiality Obligations
(March 10, 2006 through December 31, 2006)



As noted above, we examined approval ECs to determine whether the recitals required to be made when seeking to impose the non-disclosure and confidentiality obligations matched the text of the NSLs. We found that the language of the approval ECs was not consistent with the corresponding NSLs in only 2 of the 365 instances. In one instance, the approval EC did not include the SAC's certification of the need for the requirements, and in the other the approval EC contained internally inconsistent recitals about the necessity for invoking the provisions.

Of the 364 NSL approval ECs that included justifications for imposing the obligations, 225, or 62 percent, included 1 of the 13 justifications listed in the FBI OGC's March 15, 2006, guidance discussed above. Of these 225 approval ECs, 184, or 82 percent, stated that disclosure could prematurely reveal a national security investigation to the target or persons affiliated

with the target or the subject matter of the national security investigation and cause them to change their behavior patterns and circumvent detection. This justification also was cited in 23 additional approval ECs in conjunction with 7 other justifications from FBI OGC's list. The remaining 18 approval ECs cited other justifications suggested by the FBI OGC.

The balance of the approval ECs (139 of 364, or 38 percent) referred to adverse consequences from premature disclosures that were not specifically referenced on the FBI OGC's list. The adverse consequences described in the certifications ranged from perfunctory justifications to detailed descriptions of the specific consequences that might result from disclosure. The detailed descriptions included how disclosure would affect the behavior of suspects or the effectiveness of the FBI's investigative techniques and overall investigations.

Of the 364 approval ECs we examined that sought approval to impose the non-disclosure and confidentiality obligations, all but 17 (5 percent) contained justifications for imposing the non-disclosure and confidentiality obligations that complied with the FBI OGC's guidance. The remaining approval ECs contained justifications for imposing the obligations that were case-specific. Examples of these justifications were that disclosure:

> will have a detrimental effect on the instant investigation for a number of reasons. First, [redacted] and his associates would likely conceal their activities from the FBI and therefore frustrate FBI efforts to collect evidence of terrorist activity. Second, [redacted] would refrain from using the telephone to discuss [redacted] matters which would undermine FBI efforts [redacted]. Third, premature exposure of an FBI interest in [redacted] would jeopardize the terrorist financing investigation of [redacted] and possible FBI recruitment efforts.
>
> * * *
>
> Due to [redacted] communications with subjects in [redacted] who've been detained on terrorism related charges since [redacted] and his communication and association with subjects of several [full investigations], disclosure of this request may detrimentally effect [sic] the outcome of the foreign prosecutorial efforts of charged terrorists in [redacted] and ongoing intra-divisional counterterrorism investigations.

Examples of perfunctory justifications that we found to be insufficient were:

You should remind [redacted] Bank that it is prohibited from disclosing that the FBI has made this request since it may interfere with an [sic] counterterrorism investigation.

* * *

A Preliminary international terrorism investigation of subject, a Non-U.S. Person, was authorized in accordance with Attorney General Guidelines because the subject is or may be engaging, or has or may have engaged, in activities constituting a threat to the national security for or on behalf of a foreign power. The subject may or may not be involved with international terrorist activities, or knowingly conspired with or aids and abets such a person in such activities.

B. NSLs That Did Not Invoke Non-Disclosure and Confidentiality Obligations

Our review determined that 10 of the 375 NSLs we examined, or 3 percent, were issued "without the certification necessary to require the recipient of such letter[s] to comply with the nondisclosure and confidentiality requirements potentially applicable under law."[112] We reviewed the approval ECs associated with these 10 NSLs and found that 4 of these approval ECs contained representations that the facts of the cases did not warrant imposition of the non-disclosure and confidentiality obligations under the applicable NSL statute. Therefore, it appears that the absence of the non-disclosure and confidentiality provisions in the NSLs was deliberate in these four cases and not an oversight.

In contrast, 6 of the 10 approval ECs were inconsistent with the corresponding NSLs. In five instances, the non-disclosure and confidentiality provisions were not included in the NSL despite the fact that the SAC had certified the need for the requirements in the approval ECs.[113] In one instance, the approval EC failed to address the basis for the SAC's

---

[112] Patriot Reauthorization Act, § 119 (b)(3)(E).

[113] We determined that in three of the five instances the approval ECs contained the certifications justifying imposition of the non-disclosure and confidentiality obligations, but the case agents used outdated NSL models that did not contain the appropriate provisions. In two other instances, the approval ECs contained the certifications justifying imposition of the non-disclosure and confidentiality obligations, but the provisions were missing from the associated NSLs.

determination that the facts did not warrant imposition of the non-disclosure and confidentiality obligations.[114]

Based on our sample, we project that, in total, the FBI issued 405 NSLs from March 10, 2006, through December 31, 2006, that did not impose the non-disclosure and confidentiality obligations.

C. "Blanket" NSLs Issued in 2006

As noted above, in the course of our exigent letters investigation we examined 11 NSLs issued by FBI Headquarters officials in the Counterterrorism Division in connection with efforts to issue legal process to cover information already acquired through exigent letters and other informal requests.

Eight of these 11 improper NSLs imposed non-disclosure and confidentiality requirements on the recipients that did not comply with the Patriot Reauthorization Act certification requirement for invoking these provisions.[115] The individuals who prepared these NSLs appear to have relied upon outdated NSL models that did not include the required certification. These eight NSLs included the pre-Patriot Reauthorization Act language to the effect that the recipient was prohibited under 18 U.S.C. § 2709(c) from disclosing that the FBI had sought or obtained access to information or records under the ECPA.[116]

In addition, none of these 11 blanket NSLs complied with internal FBI policy requiring the preparation and approval of memoranda establishing the existence of an open investigation and the relevance of the information sought to the underlying investigation. FBI policy requires that such

---

[114] We determined that the case agent used an outdated approval EC that did not provide options for including or omitting the non-disclosure and confidentiality provisions in the NSL.

[115] The other three blanket NSLs imposed a non-disclosure requirement on the recipients that complied with the Patriot Reauthorization Act certification requirement for invoking these provisions.

As we will describe in detail in our next NSL report, we determined that five of the eight NSLs that failed to contain the required ECPA certification violated the ECPA NSL statute for two additional reasons: two of the five NSLs were signed by FBI personnel who were not authorized to sign NSLs and at least four of the five sought records that were not relevant to an investigation of international terrorism.

[116] The FBI officials who signed these NSLs were an Assistant Director, a Deputy Assistant Director, two Acting Deputy Assistant Directors, and a SAC. In addition to being non-compliant with the non-disclosure and confidentiality requirements, these NSLs were improper for other reasons that will be discussed in the OIG's forthcoming NSL report. We determined that none of these NSLs was reviewed by FBI OGC attorneys.

memoranda accompany the submission of NSLs for approval; be approved by the squad supervisor and Assistant Special Agent in Charge; and contain a statement by the official signing the NSL that non-disclosure is necessary, together with facts to justify the non-disclosure and confidentiality obligations. Since November 28, 2001, FBI policy stated that NSLs should also be reviewed by CDCs to ensure legal sufficiency.[117]

III. OIG Conclusions and Recommendation

The vast majority of the NSLs and approval ECs we examined in our random sample substantially complied with the Patriot Reauthorization Act certification requirement and FBI policy related to non-disclosure and confidentiality requirements. We believe this compliance record was largely due to the prompt guidance the FBI OGC issued on the date the Act was signed, the availability of new NSL forms on its Intranet website, and periodic guidance FBI OGC attorneys provided to the field as questions arose.

Our analysis also showed that at least 97 percent of the NSLs we examined in the random sample imposed the non-disclosure and confidentiality obligations on recipients. The majority of the approval ECs supporting these NSLs referenced the assertion that disclosure of the NSL could [redacted]. Case agents seeking approval of these NSLs for the most part adopted suggestions by the FBI OGC as to the possible adverse consequences that could result from disclosure.

In general, FBI employees complied with the requirement to provide substantive justifications for the non-disclosure certifications. We found that only 5 percent of the approval ECs in the random sample contained

---

[117] The November 28, 2001, FBI OGC memorandum states that "[p]rior to certification, every NSL and cover EC issued by the field division should be reviewed by . . . the Office of the Chief Division Counsel . . . ." The memorandum provides that "[l]awyers reviewing NSL packages should use the checklists provided with this communication to ensure legal sufficiency." Office of General Counsel, National Security Law Unit, Federal Bureau of Investigation (FBI), electronic communication to all Field Offices, National Security Letter Matters, November 28, 2001. The FBI Director's March 9, 2006, delegation memorandum authorized the NSLB to issue guidance regarding the revisions of the national security letter statutes. NSLB's Intranet website stated in 2006 that "NSLs are reviewed by CDCs at the field office level." On June 1, 2007, the FBI OGC issued a comprehensive guidance EC to all divisions for the first time stating that "all Field Office NSLs must be reviewed by CDCs or ADCs for legal sufficiency" prior to forwarding the NSLs to the SAC for approval. The comprehensive guidance EC is described in Chapter Two of this report.

perfunctory justifications for invoking the requirements. In these instances, the case agents apparently failed to read or to follow FBI guidance plainly stating that such perfunctory reasons were not satisfactory. In addition, the case agents' squad supervisors, CDCs, and SACs accepted and approved these insufficient justifications. While the number of non-compliant NSLs in our random sample was small, we are concerned that some case agents and their supervisors failed to adhere to FBI policy requiring sufficient justification for imposing non-disclosure and confidentiality requirements on NSL recipients.

Although we did not seek to verify whether the facts cited to support imposition of the non-disclosure and confidentiality obligations were accurate, we note that many of the approval ECs seeking to impose these obligations recited one of the FBI OGC's rationales without providing additional supporting details.[118] The FBI's comprehensive guidance EC dated June 1, 2007, directed that "FBI officials must make a case by case determination whether disclosure of the NSL" may cause one of the enumerated dangers to arise. We recommend that the FBI reiterate that case agents and supervisors must give individualized scrutiny to the circumstances of each case before seeking to invoke the non-disclosure and confidentiality requirements and that the FBI's Inspection Division and the Department's National Security Division consider including whether these justifications are factually supported in their periodic audits.[119]

We found that a small number of NSLs and approval ECs in our random sample (8 of 375) contained inconsistent recitals with respect to the need for invoking the non-disclosure and confidentiality obligations. Case agents and their supervisors, as well as CDCs, failed to identify and correct these errors. To address this and other data entry discrepancies, the FBI has implemented several corrective measures, including a new NSL data system that FBI officials believe will eliminate this and other data entry errors in the creation of NSLs and approval ECs.[120]

More troubling, 11 blanket NSLs issued by Headquarters officials in 2006 that sought telephone data on 3,860 telephone numbers did not

---

[118] We believe the justification required by FBI policy should be described in the approval EC and that it is not sufficient that the justification is documented elsewhere in the investigative file. Squad supervisors and CDCs (or internal and external auditors) should not be expected to search through multi-volume investigative files to locate reasons for invoking non-disclosure and confidentiality obligations. In light of the FBI OGC's June 1, 2007, comprehensive guidance EC, approval ECs must now contain facts supporting imposition of these obligations.

[119] These periodic audits are described in Chapter Two of this report.

[120] The corrective measures implemented by the FBI in response to our first NSL report are described in Chapter Two of this report.

comply with the Patriot Reauthorization Act requirements respecting these provisions, internal FBI policy, or both. We are concerned by the failure of senior Counterterrorism Division officials to comply with statutory requirements and internal policy regarding the issuance of NSLs and their failure to consult legal counsel. As noted previously, we will examine the circumstances that led to the issuance of these blanket NSLs in the OIG's forthcoming NSL report.

Based on our review and to ensure that non-disclosure and confidentiality provisions are imposed only when appropriate, we recommend that the FBI:

1. 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 and confidentiality requirements on the NSL recipient.

CHAPTER SEVEN:
IMPROPER OR ILLEGAL USE OF NATIONAL SECURITY LETTERS REPORTED BY FBI PERSONNEL IN 2006

The Patriot Reauthorization Act directed the OIG to describe "improper or illegal uses" of the NSL authorities in 2006, similar to the requirement in our first NSL report. In this chapter, we report some of our findings on improper or illegal use of NSL authorities that were identified and reported to the FBI Office of the General Counsel (FBI OGC) by FBI personnel in 2006. However, our main findings on the most serious improper or illegal uses of NSL authorities will be described in our next NSL report, which will include the results of our detailed investigation of the FBI's use of exigent letters. That investigation expanded on the results of our exigent letter review in our first NSL report by examining, among other topics, the scope of the practice; the FBI's efforts to issue legal process after the fact to cover the information obtained from the exigent letters and other improper requests; our assessment of the accountability of FBI personnel, including agents who signed exigent letters and their supervisors, for the improper use of exigent letters; and the results of our examination of improper NSLs served on three communication service providers.

As we will fully describe in our next NSL report, from 2002 through 2006, we found that the FBI obtained telephone data on approximately 3,764 domestic and international telephone numbers (which correspond to approximately 2,032 unique telephone numbers) pursuant to exigent letters and other informal requests rather than through NSLs or other legal process served in advance of obtaining the records. We also found that the FBI issued 11 "blanket" NSLs in 2006 that sought retroactively to justify the FBI's acquisition of data through the exigent letters or other informal requests. All 11 of these blanket NSLs were improper for one or more reasons. Some sought records that the FBI was not authorized to obtain through the *Electronic Communications Privacy Act* (ECPA) NSL statute; many were issued in violation of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines); and all were issued in violation of internal FBI policy. Following consultation with FBI OGC attorneys, the FBI issued new NSLs in 2007 to correct some of the improper blanket NSLs and also generated for the first time documentation explaining the predication for these NSLs.[121] In light of our findings of significant improper or illegal use of NSLs in 2006 through

[121] We will describe and evaluate in our forthcoming NSL report the FBI OGC's adjudication of any possible intelligence violations that were reported as a result of exigent letters, blanket NSLs, and other improper requests.

the use of exigent letters, other informal requests, improper blanket NSLs, and other improper NSLs, our findings in this chapter should be considered in conjunction with our forthcoming NSL report.

Chapter Three of this report describes additional improper NSLs identified through three reviews conducted by the FBI in 2007 in response to the OIG's first NSL report:

> (1) a review of NSLs issued by FBI field offices from a random sample of 10 percent of all national security investigations active at any time from 2003 through 2006;
>
> (2) a review of a random sample of 10 percent of all NSLs issued by Headquarters divisions during the same period; and
>
> (3) a review of all NSLs issued pursuant to the *Fair Credit Reporting Act* (FCRA) in counterintelligence investigations from 2002 through 2006.

In this chapter, we address the matters that were self-reported by FBI field personnel in 2006 to the FBI OGC as possible intelligence violations. These violations occurred before the OIG issued its first NSL report and before the FBI began taking corrective action in response to our report (described in Chapter Two of this report). It is therefore not surprising that we found possible NSL-related intelligence violations in 2006 comparable to our findings in our first NSL report. Moreover, compared with the number of possible intelligence violations associated with the FBI's 2007 reviews, exigent letters and other informal requests, and the 11 blanket NSLs and other improper NSLs issued in 2006, the number of matters discussed in this chapter is relatively small.

It is important to note, however, as described in Chapter Three of this report, that the overwhelming majority of possible NSL-related intelligence violations that occurred since the Patriot Act significantly expanded the FBI's NSL authorities were not reported by FBI personnel to the FBI OGC through the self-reporting mechanism established 25 years ago to identify and address such violations.[122]

As described in Chapter Two of this report, the FBI is in the process of implementing the recommendations in our first NSL report that were intended to improve its compliance with NSL statutes, Attorney General Guidelines, and internal FBI policy. Moreover, the FBI and other components of the Department are taking additional steps to promote

---

[122] Possible intelligence violations can be reported by case agents, the case agents' supervisors who approve the issuance of the NSLs, or the Chief Division Counsels (CDC). They also can be reported as a result of a supervisor's file review or an audit.

compliance with NSL statutes and policies governing other investigative techniques used in national security investigations. Once implemented, the FBI believes that many of the errors categorized as possible intelligence violations in our first NSL report, in the FBI's 2007 reviews, and in this chapter will be significantly reduced.

In Section I of this chapter, we describe the FBI's procedures for reporting possible Intelligence Oversight Board (IOB) violations to the FBI OGC and the FBI OGC's process for deciding whether to report the violation to the IOB. In Section II, we discuss violations triggered by the use of NSLs that were reported in 2006 by case agents to the FBI OGC as possible violations that should be reported to the IOB. In Section III, we summarize our conclusion and provide our recommendations.

As we did in our first NSL report, we determined whether the FBI would have been entitled to the information under applicable NSL statutes, Attorney General Guidelines, and internal policies. We found that of the 84 possible intelligence violations identified and reported to the FBI OGC in 2006, the FBI received information it was not entitled to receive in 14 matters. In one of the matters the FBI requested information it was not entitled to under the applicable NSL statute. In this matter the case agent modified the standard language used for requesting information pursuant to the ECPA NSL statute by requesting publicly available content information. The FBI OGC concluded that the alteration of the ECPA NSL statutory language to request and obtain the information was beyond the scope of the ECPA.[123]

In the other 13 matters, the FBI made proper requests but, due to third party errors, obtained information it was not entitled to receive under the pertinent NSL statutes.

---

[123] We could not conclude whether the FBI compounded the errors involved in 52 matters in which it received unauthorized information as a result of third party errors because the FBI OGC has not yet adjudicated whether the FBI used the inappropriately obtained information or uploaded it into FBI databases. Prior to November 13, 2006, case agents were required to report to the FBI OGC unauthorized collections from third party errors. Effective November 13, 2006, the IOB agreed that such third party errors did not have to be reported to the IOB. However, as discussed later in this chapter, on August 1, 2007, the IOB directed that the FBI report unauthorized collections due to third party errors if the FBI compounded the errors by using information inappropriately provided or uploading it into FBI databases. We consider matters in which the FBI compounded third party errors to be an "improper" use of NSL-derived information.

I. The FBI Process for Reporting Possible Violations Involving Intelligence Activities in the United States

In this section we briefly summarize the FBI's procedures for reporting possible intelligence violations to the FBI OGC and the manner in which the FBI OGC decides whether to report possible intelligence violations to the IOB. We then describe the November 2006 FBI OGC guidance to the field on reporting possible intelligence violations to the FBI OGC and separate guidance to the FBI OGC attorneys assigned to evaluate possible intelligence violations.

A. The Process for Reporting Possible Intelligence Violations

Executive Order 12863 designates the IOB as a standing committee of the President's Foreign Intelligence Advisory Board and directs the IOB to inform the President of any activities that "may be unlawful or contrary to Executive Order or Presidential Directive."[124] This directive has been interpreted by the Department and the IOB during the period covered by our review to include reports of possible violations of provisions of Attorney General's NSI Guidelines or other guidelines or regulations approved by the Attorney General in accordance with Executive Order 12333, dated December 4, 1981, if the provision was designed to ensure the protection of individual rights.

To comply with the Executive Order 12863 directive, the FBI has developed an internal process for reporting possible intelligence violations to the FBI OGC that begins with the duty of FBI personnel to self-report to the FBI OGC possible intelligence violations within 14 days of discovery. These reports must include the identification of the substantive investigation in which the questionable activity occurred, the names of the relevant FBI personnel, the identification of the investigation's subject's status as a U.S. person or non-U.S. person, the legal authority for the investigation, a complete and thorough explanation of the error believed to have been committed, and the date of the incident. FBI OGC attorneys review the reports, prepare a written opinion as to whether the matter should be reported to the IOB, and draft the written communication to the IOB for those matters the FBI OGC determines meet the reporting requirements of Executive Order 12863.

In November 2006, the FBI OGC issued guidance to the field on the types of infractions involving the use of NSLs that must be reported to the

---

[124] For a more detailed description of the IOB reporting process, see Office of the Inspector General, *Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act* (March 8, 2006).

FBI OGC as possible intelligence violations. The FBI OGC also issued revised guidance for attorneys assigned to its National Security Law Branch (NSLB) who evaluate possible intelligence violations. These guidance memoranda are described below.

B. FBI Guidance on Reporting and Adjudicating Possible Intelligence Violations

1. November 16, 2006, Guidance on Reporting Possible IOB Violations to the FBI OGC

On November 16, 2006, the FBI OGC issued a memorandum to all FBI divisions regarding revised procedures for reporting possible intelligence violations.[125] Although the FBI OGC previously had issued general guidance on reporting possible intelligence violations and responded informally to questions that arose from the field about matters that should be reported, it had not previously identified in a comprehensive manner what infractions relating to the use and approval of NSLs (or other investigative techniques) were required to be reported to the FBI OGC and the Inspection Division's Internal Investigations Section as possible intelligence violations.[126] The November 16, 2006, guidance also addressed the FBI's retention practices for handling improperly or unintentionally acquired information and reporting such matters to the FBI OGC. As we noted in our first NSL report, prior to the 2006 guidance, FBI practices regarding these issues were not uniform, and the guidance for FBI employees was not clearly articulated.[127]

The memorandum identified the following types of NSL-related incidents that must be reported to the FBI OGC as possible intelligence violations and cautioned that the list was not exhaustive:

> Serving a National Security Letter (NSL) that contains a substantive typographical error that results in the acquisition of data that is not relevant to an authorized investigation (i.e., numbers in telephone number transposed).

---

[125] Office of the General Counsel, National Security Law Branch (NSLB), Federal Bureau of Investigation, electronic communication to all divisions, Revised Procedures for the Submission of Reports of Potential Intelligence Oversight Board Matters, November 16, 2006.

[126] On April 7, 2006, the FBI OGC sent an e-mail to all CDCs and NSLB attorneys stating that unauthorized collections due to third party errors should be reported to the FBI OGC as possible intelligence violations. That policy was formalized and disseminated to all FBI divisions on November 16, 2006.

[127] See NSL I, 29.

Serving an NSL that requests information that is beyond the scope permissible by statute (i.e., content information).

Receiving information from a carrier beyond the scope of an NSL resulting in the unintentional acquisition of data.

The memorandum also directed FBI personnel to sequester with each field division's Chief Division Counsel (CDC) any information improperly received or unintentionally acquired using an NSL.[128] The memorandum stated that as part of its IOB adjudication process, the National Security Law Branch (NSLB) will advise the field whether the information may be used or whether it must be returned to the carrier or be destroyed with appropriate documentation to the file.

2. November 30, 2006, Guidance to FBI OGC NSLB Attorneys Adjudicating Possible IOB Violations

On November 30, 2006, the FBI OGC issued guidance to FBI OGC attorneys assigned to draft opinions based on reports of possible intelligence violations.[129] The memorandum described whether certain matters reportable to the FBI OGC in turn should be reported to the IOB. The categories addressed in the guidance were certain violations of the Attorney General's NSI Guidelines, conduct involving NSLs, mistakes involving information obtained pursuant to orders of the Foreign Intelligence Surveillance Court, and conduct pertaining to other investigative techniques authorized by the Attorney General's NSI Guidelines.

With respect to the use of NSLs, the guidance directed FBI OGC attorneys to review the attachment to the NSL to determine whether there had been an unauthorized collection.[130] The guidance further stated that if the information obtained in response to an NSL was referenced in the attachment to the NSL, it was not necessary for the field to report the matter to the FBI OGC and the Inspection Division. If the information was not referenced in the attachment but was relevant to the investigation, the CDCs in the field office that issued the NSL were directed to sequester the

---

[128] National Security Law Branch, electronic communication to all divisions, November 16, 2006. The FBI OGC further directed that information unintentionally acquired under the *Foreign Intelligence Surveillance Act* be sequestered, sealed, and delivered to the responsible FBI Headquarters unit to be submitted to the Foreign Intelligence Surveillance Court for appropriate disposition. Id.

[129] Julie Thomas, Deputy General Counsel, NSLB, Federal Bureau of Investigation, memorandum to NSLB Attorneys, Guidance for Drafting IOB Opinions, November 30, 2006.

[130] FBI practice is to list on an attachment to the NSL – rather than in the body of the NSL itself – the types of records that the recipient may consider to be within the scope of the statute.

information until a new NSL was issued for the information. However, the guidance directed that such matters were to be reported to the FBI OGC and the Inspection Division as possible intelligence violations.

The most significant issue addressed in the guidance memorandum was whether information obtained by the FBI that was beyond the scope of the NSL due to third party error – referred to as "unauthorized collections" – had to be reported to the IOB. The memorandum advised that "if the FBI properly issues an NSL, and the carrier provided the information outside the scope of the NSL, the matter is not reportable to the IOB."[131] However, the memorandum did not address whether the FBI's handling of the unauthorized information could in some circumstances trigger the need to report to the IOB. For example, guidance did not address whether, if case agents received and uploaded unauthorized information provided to the FBI due to third party error, the mishandling of such information should be reported to the IOB.

On August 1, 2007, the IOB directed the FBI OGC to report third party errors that are compounded by the FBI.[132] Upon such direction, FBI OGC officials told us that they began evaluating third party errors to determine if the FBI compounded the errors by using the inappropriately provided information or uploading it into FBI databases. As a result of the new directive, the FBI OGC said it would reevaluate reports of unauthorized collections to determine if the FBI compounded the initial third party errors. If so, FBI OGC officials told us they would report the matters to the IOB.

II. Possible Intelligence Violations Arising From National Security Letters Reported to the FBI OGC in 2006

We determined that in 2006 FBI field divisions reported 84 possible intelligence violations to the FBI OGC arising from the use of NSL authorities in 75 different national security investigations.[133] As shown in Chart 7.1, this compares with 26 possible intelligence violations reported to

---

[131] The November 30, 2006, memorandum noted that the IOB had agreed that third party errors that resulted in the unauthorized collection of information pursuant to an NSL must be reported to the FBI OGC but were not required to be reported to the IOB. See General Counsel, Intelligence Oversight Board, letter to Julie F. Thomas, Deputy General Counsel, NSLB, Federal Bureau of Investigation, November 13, 2006.

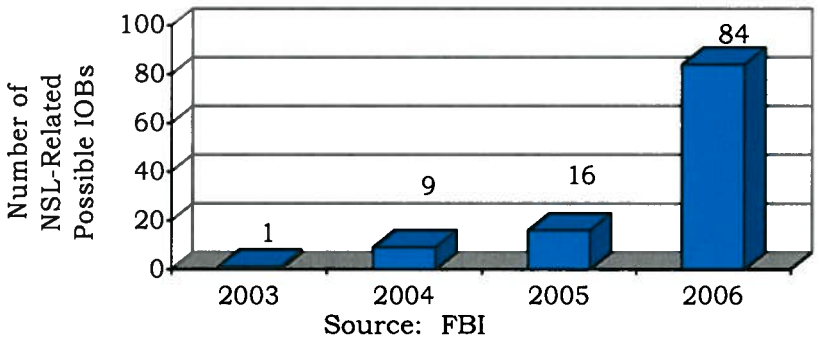
[132] See General Counsel, Intelligence Oversight Board, letter to Julie F. Thomas, Deputy General Counsel, NSLB, Federal Bureau of Investigation, August 1, 2007.

[133] We considered the universe of possible NSL-related intelligence violations in 2006 to include all matters reported to the FBI OGC between January 1, 2006, and December 31, 2006. We reviewed all such matters for which we received documentation by August 1, 2007.

the FBI OGC over a 3-year period (2003 through 2005) as we reported in our first NSL report.[134]

We believe the overall increase in the reports of possible intelligence violations may be explained in large part by the attention that our first NSL review focused on the FBI's obligation to examine information obtained in response to NSLs and report possible intelligence violations and closer scrutiny of NSLs and NSL-derived information by case agents, supervisors, and CDCs.

CHART 7.1
Possible NSL-Related IOB Violations Reported to the FBI OGC (2003 through 2006)



Source: FBI

FBI Headquarters divisions, which issued approximately 450 NSLs in 2006, reported, in conjunction with a field office, one possible NSL-related intelligence violation to the FBI OGC in 2006.[135] Headquarters divisions did not report any such violations from 2003 through 2005.

In this section we describe the possible intelligence violations regarding the use of NSL authorities that were reported to the FBI OGC in 2006, the number and nature of the possible intelligence violations, and our analysis of these matters compared with the 26 possible intelligence

---

[134] See NSL I, 70.

[135] Based on the results of the FBI Inspection Division's review of 10 percent of the NSLs issued by Headquarters during the period 2003 through 2006, described in Chapter Three of this report, we believe that FBI Headquarters divisions were not recognizing or reporting possible NSL-related intelligence violations throughout this period. The Inspection Division review identified, based on guidance provided by the FBI OGC, at least 130 possible NSL-related intelligence violations from FBI Headquarters divisions in investigations open from 2003 through 2006. These included NSLs that exceeded statutory authority, NSLs issued solely out of control files, NSLs issued despite the lack of predication in the approval memoranda, and NSLs that resulted in unauthorized collections due to FBI or third party errors.

violations reported by the FBI from 2003 through 2005 and described in our first NSL report. Table 7.1 lists the categories of the possible intelligence violations reported in 2006 and whether they initially resulted from FBI or third party errors.[136]

TABLE 7.1
Summary of 84 Possible NSL-Related IOB Violations Reported to the FBI OGC (2006)

Category of Possible IOB Violations	Possible IOB Violations Reported to the FBI OGC		IOB Violations Reported to the IOB	
	FBI Error	Initial Third Party Error	FBI Error	Initial Third Party Error
Improper authorization	3	0	3	0
Improper request	3	0	1	0
Unauthorized investigative activity during lapse in investigation	8	0	1	0
Unauthorized dissemination	1	0	0	0
Unauthorized collection	18	52	15	14
Total Possible IOB Violations Reported to the FBI OGC in 2006	**84[137]**		**34**	

A. Possible NSL-Related IOB Violations Reported to the IOB in 2006

In 2006, the FBI OGC reported 34 of the 84 possible intelligence violations to the IOB, or 40 percent of the total.[138] Twenty of the possible intelligence violations reported to the IOB were attributable to FBI errors, while 14 were initially attributable to third party errors.

Table 7.2 provides additional details on these matters.

---

[136] In Table 7.1 and elsewhere in this chapter we use the phrase "initial third party error" because, as noted above, the FBI OGC has not yet determined whether the FBI compounded the NSL recipients' errors by using the information or uploading it into FBI databases.

[137] One matter included an initial third party error that resulted in both an unauthorized collection and an improper request by the FBI. Both possible intelligence violations are reflected in Table 7.1.

[138] Possible intelligence violations reported to the FBI OGC are also reported to the Inspection Division's Internal Investigations Section (IIS). If IIS determines that the conduct of an FBI employee is more than a performance issue, the FBI OGC refers the matter to the FBI's Office of Professional Responsibility (FBI OPR). The FBI Inspection Division reported that it did not refer any reports of these possible violations to the FBI OPR in 2006.

TABLE 7.2
Summary of 34 NSL-Related IOB Violations Reported to the IOB by the FBI OGC (2006)

Category of IOB Violations	Number of Violations Reported to the IOB
Improper Authorization (FBI Error)	
Issuing ECPA NSL without obtaining required Special Agent in Charge authorization to extend preliminary investigation after 6 months	1
Issuing Right to Financial Privacy Act (RFPA) NSL without obtaining required Headquarters authorization to extend preliminary investigation after 1 year	1
Serving ECPA NSLs before preliminary investigation was properly reauthorized by Special Agent in Charge	1
Improper Request (FBI Error)	
Issuing ECPA NSL to an Internet service provider in a manner that was deemed an improper request under pertinent NSL statute	1
Unauthorized Investigative Activity During Lapse in Investigation After NSL Was Properly Issued (FBI Error)	
Obtaining and analyzing RFPA records without obtaining required FBI Headquarters authorization to extend preliminary investigation after 1 year[139]	1
Unauthorized Collection (FBI Error)	
Obtaining ECPA telephone subscriber information not relevant to an authorized national security investigation	3
Obtaining ECPA telephone toll billing information not relevant to an authorized national security investigation	10
Obtaining ECPA e-mail subscriber information not relevant to an authorized national security investigation	1
Obtaining ECPA electronic communication transactional records not relevant to an authorized national security investigation	1
Total FBI Errors	**20**[140]

[139] In November 2007, the FBI OGC advised the OIG that it intends to issue a corrected adjudication memorandum stating that this violation is not reportable to the IOB.

[140] The four possible NSL-related intelligence violations in Table 7.2 that are categorized as improper authorizations and improper requests also resulted in unauthorized collections. However, we did not "double count" these matters by including them in the "unauthorized collection" category.

Category of IOB Violations	Number of Violations Reported to the IOB
Unauthorized Collection (Initial Third Party Error)[141]	
Obtaining ECPA telephone subscriber information not relevant to an authorized national security investigation	2
Obtaining ECPA telephone toll billing information not relevant to an authorized national security investigation	4
Obtaining ECPA telephone toll billing information outside the time frame requested in the NSL	2
Obtaining subject line or full content in response to an electronic communication transactional record ECPA NSL	3
Obtaining ECPA e-mail subscriber information not relevant to an authorized national security investigation	1
Obtaining RFPA financial records not relevant to authorized national security investigation	2
Total Initial Third Party Errors	**14**
Total Number of Violations Reported by the FBI OGC to the IOB	**34**

Nature of IOB Violations: The 34 intelligence violations reported by the FBI to the IOB in 2006 involved the following categories of violations.

- In three matters NSLs were signed by appropriate field officials but the underlying investigations had not been approved or extended by the appropriate Headquarters or field supervisors.
- In one matter an NSL was served on an Internet service provider (ISP) in a manner that that was deemed an improper request under the pertinent NSL statute.

[141] As noted previously, "unauthorized collections" is a phrase used by the FBI and the OIG to describe several circumstances in which the FBI receives information in response to NSLs that was not requested or was mistakenly requested. For example, many unauthorized collections occur due to errors on the part of NSL recipients when they provide more information than was requested (such as records for a longer period of time or records on additional persons). The FBI sometimes also refers to these matters as "over collections" or "overproductions." We refer to these as "initial third party errors" because, while the NSL recipient may initially have provided more information than requested, the FBI may or may not have compounded the initial error by using or uploading the information. Other unauthorized collections can result from FBI errors, such as when a typographical error in the telephone number or e-mail address results in the acquisition of data on the wrong person or e-mail address. When we present data on "unauthorized collections" in this report we note whether the infraction occurred due to initial third party error or FBI error.

- In one matter the NSL was appropriately issued but the NSL recipient provided the records after the preliminary investigation had lapsed.
- In 29 matters the NSL recipient provided information that was not requested in the NSL or provided information on the wrong person due either to FBI typographical errors or initial errors by the NSL recipients.[142]

Three of the 14 initial third party errors noted in Table 7.2 resulted in the FBI's acquisition of either full e-mail content (two matters) or e-mail subject line content (one matter) from ISPs in response to ECPA electronic communication transactional record NSLs. In the two matters that resulted in acquisition of full e-mail content, an ISP mistakenly provided on the same disk the full message content of the e-mails for the requested account and for the account of an associated subscriber in the same investigation whose records had been requested in another NSL. On instruction from the FBI OGC, the disk and paper copies of the records were sealed and sequestered by the field division's CDC, and a new NSL was issued. In response, the ISP improperly sent the same full content information, which was thereafter again sequestered.

In the matter involving acquisition of e-mail subject line content, the ISP included the subject field for each e-mail transaction along with the e-mail header information for the requested 2-year time period. The NSL specifically directed that the ISP not include subject fields in its response. The FBI OGC directed that the information that exceeded the scope of the NSL be sealed and sequestered and await further direction from the FBI OGC.

Status of Investigative Subject and Target of NSL: We also attempted to determine whether the subject of the investigation in these 34 matters was a U.S. person and if the investigative subject was the same as the target of the NSL.[143]

---

[142] Of the 15 unauthorized collections resulting from FBI errors, 12 were due to typographical errors, 2 were due to inadvertent misidentification of telephone numbers, and 1 was due to a computer software mistake.

[143] 50 U.S.C. § 1801(i) defines a "United States Person" as:

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

On June 1, 2007, the FBI OGC issued comprehensive guidance that reiterated earlier guidance instructing agents to identify in NSL approval documents the status of

(Cont'd.)

- In 25 of the 34 matters, the subject of the investigation was a U.S. person, in 8 matters the subject was a non-U.S. person, and in 1 matter the status of the subject could not be determined.
- In 27 of the matters, the NSLs sought information about the subject of the underlying national security investigation, 3 NSLs sought information on a person other than the subject, 1 NSL sought information on both the subject and a non-subject; and 3 NSL targets could not be determined.

Timeliness of Reporting: We determined that 19 of the 34 possible intelligence violations reported to the IOB (56 percent) were reported within 14 days of discovery to the FBI OGC in accordance with FBI policy. However, 12 (35 percent) were not reported in a timely fashion.[144] Seven of these 12 took between 17 and 46 days to report and 5 took between 145 and 418 days. In two of these five matters, the agents did not realize the matters were reportable as possible intelligence violations until they attended NSL training a year after the violations occurred.[145] In the other three, no reason was given for the delay in reporting. We could not determine how long it took to report the remaining 3 of the 34 violations.

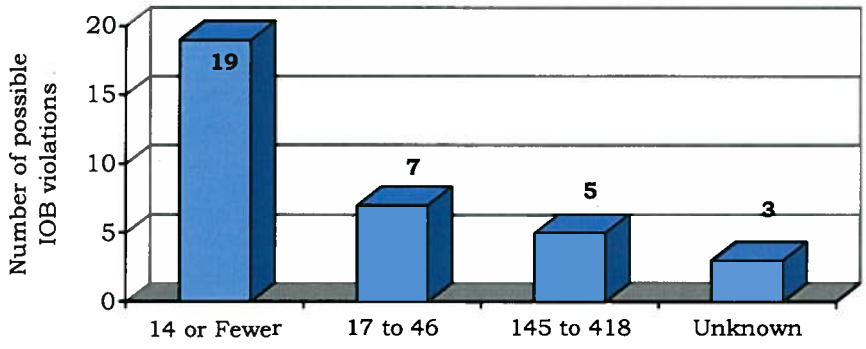
---

persons associated with all NSL requests. See National Security Law Policy and Training Unit, Federal Bureau of Investigation, electronic communication to all divisions, Comprehensive Guidance on National Security Letters, June 1, 2007, at 13, which we described in detail in Chapter Two of this report.

[144] This compares with 6 of the 26 possible intelligence violations (23 percent) reported in 2003 through 2005 that were not reported to the FBI OGC within 14 days of discovery, described in our first NSL report. See NSL I, 74.

[145] In both matters, the agents made typographical errors in the NSLs and discovered the errors when they received the records from the NSL recipients.

CHART 7.2
Timeliness of 34 FBI Field Reports to the FBI OGC of Possible NSL-Related IOB Violations Reported to the IOB (2006)



Source: FBI

We also calculated the time it took for FBI personnel to identify possible intelligence violations. From our examination of reports to the FBI OGC, we determined that 26 of the 34 violations were discovered within approximately 2 months of the occurrence. Five of the possible intelligence violations were discovered between approximately 2 months and 8 months after they occurred. In one instance, discovery was delayed because the case agent mistakenly believed the underlying preliminary investigation had been extended. In the second case, discovery did not occur until the data was being uploaded into an FBI database. In the third, the case was reassigned and the violation not discovered until the new case agent took over. In the two remaining cases, field reports to the FBI OGC did not specify reasons for the delay. We could not determine how long it took for FBI personnel to discover the remaining three possible violations.

Remedial Actions: Twenty-nine of the 34 possible NSL-related intelligence violations reported to the IOB in 2006 involved unauthorized collections. We examined the 29 matters to determine whether case agents handled the unauthorized information in conformity with FBI guidance. FBI field and FBI OGC documentation stated that the inappropriately obtained records received in response to 20 of these 29 matters were sealed and sequestered while they were awaiting final dispositions by the field offices or further instructions from the NSLB. In field reports to the FBI OGC for the remaining nine matters, documentation indicated that a variety of remedial steps were taken: issuing a new NSL for the records; forwarding the unauthorized material to FBI Headquarters for appropriate action; offering the records back to the NSL recipient; removing telephone data from Telephone Applications, the FBI's principal database for storing telephone records, and from other FBI records; and destroying the records.

Twenty-one of the 29 matters reported to the FBI OGC involving unauthorized collections resulted in the FBI's acquisition of telephone subscriber or toll billing records. We examined the field reports to the FBI OGC to determine whether the inappropriately obtained data was uploaded into FBI databases. While 17 of the 21 reports stated that the information was not uploaded, we found that field reports for 4 matters did not address the issue.

B. OIG Analysis Regarding Possible NSL-Related IOB Violations Reported to the IOB

As we found in our first NSL report, the severity of the possible intelligence violations reported to the IOB varied. We believe the most serious were those in which the FBI obtained full e-mail content. In 2 of the 14 instances in which the unauthorized collection was initially attributable to third party errors, the FBI received full content e-mail information.[146] Among the 15 matters in which the FBI collected unauthorized information due to FBI error, 10 were due to typographical errors or misidentification of telephone numbers that resulted in the FBI collecting telephone toll records on the wrong person.

Our examination of the 34 possible NSL-related intelligence violations reported by the FBI to the IOB in 2006 did not evidence deliberate or intentional violations of NSL statutes, Attorney General Guidelines, or internal FBI policy. Although the majority of the possible intelligence violations – 20 of 34, or 59 percent – arose from FBI errors, most were a consequence of errors in the telephone number listed in the NSL. In all but one instance, the FBI would have been entitled to obtain the information under the NSL statutes had it followed the requirements of those statutes, Attorney General Guidelines, and internal FBI policies. In one matter, the case agent modified the standard language used for requesting information pursuant to the ECPA NSL statute by requesting publicly available content information. The FBI OGC concluded that the alteration of the ECPA NSL statutory language to request and obtain the information was beyond the scope of the ECPA. The FBI OGC concluded that the matter should be reported to the IOB because the ECPA "does not have a 'catch-all' authority, nor does it allow for content as requested in the NSL."

However, although the 14 unauthorized collections were reported to the IOB, the FBI OGC has not yet adjudicated whether case agents

[146] According to FBI records, FBI personnel did not compound the third party errors in either of these matters.

compounded the errors by using the inappropriately provided information or uploading it into FBI databases.[147]

C. Possible NSL-Related IOB Violations Not Reported to the IOB in 2006

In 2006, FBI field offices reported 50 possible intelligence violations to the FBI OGC that were not reported to the IOB. Of these 50 that were not reported to the IOB, 13 resulted from FBI errors and 38 resulted from initial third party errors.[148]

Table 7.3 provides additional details on the nature and source of these possible intelligence violations:

TABLE 7.3
Summary of 50 Possible NSL-Related IOB Violations Not Reported to the IOB (2006)

Category of Possible IOB Violations	Number of Possible Violations Reported to the FBI OGC
Unauthorized Investigative Activity During Lapse in Investigation After NSL Properly Issued (FBI Error)	
Reviewing records obtained from an ECPA NSL after the national security investigation had lapsed	1
Requesting (but not issuing or serving) an NSL after the national security investigation had lapsed	1
Allowing the national security investigations to lapse before records sought in the NSLs were received	3
Allowing the national security investigations to lapse before analyzing records obtained from RFPA or ECPA NSLs	2
Improper Request (FBI Error)	
Issuing ECPA NSL without language regarding non-disclosure and confidentiality requirements pursuant to the Patriot Reauthorization Act	1
Issuing ECPA NSLs based on an unauthorized collection	1

[147] The FBI OGC has been adjudicating over 1,200 possible IOB violations reported to it as a result of the three reviews the FBI conducted in response to the OIG's first NSL report. These reviews are described in Chapter Three of this report.

[148] One of the 50 violations included both an initial third party error and a subsequent FBI error.

Category of Possible IOB Violations	Number of Possible Violations Reported to the FBI OGC
Unauthorized Collection (FBI Error)	
Obtaining ECPA telephone subscriber information not relevant to an authorized national security investigation	1
Obtaining ECPA telephone toll information not relevant to an authorized national security investigation	2
Unauthorized Dissemination (FBI Error)	
Providing ECPA telephone subscriber and toll information to a third party not authorized to receive such information	1
Total FBI Errors	**13**
Unauthorized Collection (Initial Third Party Error)	
Obtaining ECPA telephone subscriber information not relevant to an authorized national security investigation	1
Obtaining ECPA telephone subscriber information outside the time frame or not requested in the NSL	2
Obtaining ECPA telephone toll information not relevant to an authorized national security investigation	12
Obtaining ECPA telephone toll information outside the time frame or not requested in the NSL	4
Obtaining ECPA telephone toll information when subscriber information was requested and obtaining toll records outside the time frame requested	1
Obtaining subject line or full content in response to ECPA electronic communication transactional records NSL	6
Obtaining ECPA electronic communication transactional records outside the time frame or not requested in the NSL	4
Obtaining RFPA financial records not relevant to an authorized national security investigation	3
Obtaining FCRAv full credit information in response to a FCRAu NSL in a counterintelligence investigation	4
Obtaining electronic communication transactional records in response to a preservation letter (not an NSL)	1
Total Initial Third Party Errors	**38**
Total Number of Possible NSL-Related Violations Reported to the FBI OGC and Not Reported to IOB	**51**[149]

We determined that 30 of the 50 possible intelligence violations that were not reported to the IOB (60 percent) were reported to the FBI OGC within 14 days of discovery in accordance with FBI policy. We could not determine how long it took to report 4 of the 50 possible intelligence violations. However, the remaining 16 possible intelligence violations

[149] One matter included both an unauthorized collection error by the NSL recipient and a subsequent improper request error by the FBI. Both errors are reflected in Table 7.3.

(32 percent) were not reported to the FBI OGC in a timely fashion. Eight of these 16 took between 16 and 51 days to report, and 8 took between 71 and 268 days to report.

In 12 of the 16 matters that were not reported on a timely basis, no reason was given for the delay in reporting. In 3 of the 16, the reason for the delay was that the case agents did not realize the matters were reportable as possible intelligence violations until they were informed later or until they attended NSL training.[150] In the final instance, the case agent stated that he could not ask about the possible intelligence violation until the CDC returned to the office.

D. OIG Analysis of Possible NSL-Related IOB Violations Not Reported to the IOB

Similar to possible intelligence violations reported to the IOB in 2006, the matters not reported to the IOB in 2006 varied in seriousness. Among the three possible intelligence violations not reported to the IOB in which the FBI collected information not associated with an investigation due to FBI errors, two were matters in which the FBI in good faith requested telephone records on persons they believed were associated with the telephone numbers. However, after the records were received, the case agent discovered that the two sources had provided the wrong numbers. The third possible intelligence violation was the result of a mistranslation of a foreign name. In 6 of the 38 instances in which the unauthorized collection initially was attributable to third party errors, the NSL recipients sent the FBI subject line or full content e-mail information, which is prohibited by the ECPA NSL statute. In three matters the NSL recipients sent the FBI information well beyond the time frame requested in the NSL, which resulted in collection of records 1 year, 3 years, and 4 years outside the requested time frame.

In our examination of FBI OGC decisions that resulted in determinations not to report possible intelligence violations to the IOB, we agreed with the FBI OGC's reasoning for not reporting 44 of the 50 matters. Among the six other matters, we identified four FBI OGC decisions in which the rationale for not reporting the possible intelligence violation to the IOB was inconsistent with prior FBI OGC decisions and two FBI OGC decisions that were unpersuasive. Three of these possible intelligence violations were attributable to FBI error, two resulted from third party errors, and one involved both a third party error and an FBI error.

---

[150] In each of these three instances, the NSL recipient provided records not requested in the NSL, which the case agents discovered when they received the records from the NSL recipient.

We concluded that the FBI OGC's decision not to report the following four matters to the IOB was inconsistent with other FBI OGC decisions in 2006 that involved similar facts. The four matters were:

- two third party errors in which properly served NSLs for ECPA telephone subscriber and electronic communication transactional records resulted in the acquisition of records outside the time period requested (in one instance resulting in the acquisition of records 4 years prior to the initial date noted in the NSL);[151] and
- two FBI errors in which the records obtained from properly issued NSLs (ECPA and another statute not identified) were received and analyzed prior to an authorized extension of the investigation.

For each of these four possible intelligence violations, the OIG found at least one nearly identical matter that the FBI OGC decided to report to the IOB in 2006.[152] The FBI OGC decision memoranda did not identify any facts or circumstances that distinguished these matters from similar matters that the FBI reported to the IOB in 2006.

We also identified two other matters that we believe should have been reported to the IOB under the applicable reporting standard:

---

[151] Although, as noted above, third party errors did not have to be reported to the IOB from November 13, 2006, to August 1, 2007. The two possible intelligence violations involving third party errors were adjudicated prior to those dates (October 3, 2006, and October 7, 2006). Therefore, we believe both of these should have been reported to the IOB in accordance with applicable standards at the time. The FBI OGC advised the OIG in December 2007 that it is re-evaluating these two opinions in accordance with the IOB's November 13, 2006, letter and the August 1, 2007, directive. Under the new standard, one of these two matters would be reportable to the IOB because the FBI compounded the error, and the FBI OGC told us that it will issue a corrected opinion.

[152] Similar matters that were reported to the IOB included receiving records outside the time period requested and analyzing records prior to a required extension of the investigation. In November 2007, FBI OGC officials advised the OIG that it reconsidered one of its prior decisions to report a violation to the IOB that the OIG used to contrast FBI OGC decisions not to report similar matters to the IOB. The FBI OGC stated that it had erroneously analyzed and reported a matter to the IOB in which investigative activity (specifically, analyzing records) was performed after the preliminary investigation had expired. In contrast to the reasoning of a June 2006 decision, the FBI OGC reasoned that investigative activity undertaken after the expiration of a preliminary investigation is permissible if that activity is permissible under a threat assessment pursuant to the Attorney General's NSI Guidelines. FBI OGC officials told us that they consider the NSL-derived information to be FBI records because the field office had received the records in response to a properly issued NSL. The FBI OGC's rationale is reflected in the November 30, 2006, guidance to NSLB attorneys.

- improperly disseminating records to a communication service provider received in response to an ECPA NSL seeking telephone toll billing records; and
- using data obtained through an unauthorized collection to improperly generate ECPA NSLs for telephone toll billing and electronic communication subscriber records.

In the first matter, an FBI field office obtained ECPA telephone toll billing records with the intent of sending the records to the field office that issued the NSL. Instead, the FBI field office inadvertently disseminated the records to another communication service provider rather than the field office that initiated the NSL. Documentation of the incident states that the communication service provider that received the records recognized the error and contacted the original communication service provider, which then contacted the FBI. The FBI OGC reasoned that improper dissemination to a private communication service provider did not damage national security and had no impact on the rights of the subscriber.

Although the dissemination was inadvertent and the communication service provider did not further disseminate the information, we believe any dissemination to a party not authorized to receive the records, absent the consent of the person who the records concern or in specified emergency situations, should be reported to the IOB.[153] The ECPA states that the FBI may disseminate information only as specified in the Attorney General's NSI Guidelines. The Attorney General's NSI Guidelines provide standards and procedures for the sharing and dissemination of information obtained in national security investigations. The dissemination that took place in this matter was not among the specified types of dissemination permitted by the Attorney General's NSI Guidelines, and the matter should have been reported to the IOB.[154]

---

[153] The *Electronic Communications Privacy Act*, 18 U.S.C.§ 2709(d), provides:

> The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

[154] The Attorney General's NSI Guidelines provide:

> a. Information may be disseminated with the consent of the person whom the information concerns, or where necessary to protect life or property from threatened force or violence, otherwise necessary for the safety or security of persons or property or for the prevention of crime, or necessary to obtain information for the conduct of a lawful investigation by the FBI.

(Cont'd.)

In the second matter, the FBI properly served an NSL for electronic communication (e-mail) subscriber records. In response, the NSL recipient provided the subscriber records and, in addition, electronic communication transactional records that were not requested in the NSL. Using information contained in the records that were not requested in the NSL and to which it therefore was not entitled, the FBI issued NSLs for ECPA telephone toll billing and electronic communication subscriber records (e-mail records) to two other NSL recipients. The first NSL recipient responded that it had no information, and the second NSL recipient furnished subscriber information. The FBI realized the error and issued two new NSLs to cover the information provided in response to the NSLs based on the inappropriately collected information. The field office reported the unauthorized collection and the issuance of the NSLs to the FBI OGC.

However, in its decision memorandum the FBI OGC addressed only the third party unauthorized collection, stating that the field office should contact the ISP and ask whether unintentionally acquired information should be returned or destroyed or, alternatively, issue a new NSL for the electronic communication transactional records. The FBI OGC reasoned that the original NSL was properly served, but that the provider furnished records that were not requested. Yet, the FBI OGC decision did not address the FBI's issuance of the two ECPA NSLs based on e-mail address information that the FBI had not requested in the original NSL but that was produced as a result of the NSL recipient's error. Since the FBI was not authorized to obtain the electronic communication transactional records in response to the initial NSL, we believe that the FBI's use of these records to generate additional NSLs should have been reported to the IOB as improper requests. We also believe the FBI's issuance of the NSLs that were based on the unauthorized information should also have been reported to the FBI OGC and in turn to the IOB as improper requests because the FBI compounded the third party error by using the information in its investigation.[155]

---

b. Information that is publicly available or does not identify United States persons may be disseminated for any lawful purpose.

c. Dissemination of information provided to the FBI by other Intelligence Community agencies is subject to applicable agreements and understandings with such agencies concerning the dissemination of such information.

NSI Guidelines, § VII(B)(1).

[155] The FBI improperly requested the two ECPA NSLs between March 2006 and May 2006.

(Cont'd.)

In addition to the matter described above, there were 37 other possible intelligence violations for a total of 38 matters that involved unauthorized collection due to third party errors in which the case agents may have compounded the errors. As noted in the previous section on possible intelligence violations reported to the IOB, the FBI OGC has not yet determined whether case agents compounded the third party errors in these 38 unauthorized collections.

We also examined the remedial actions taken regarding the unauthorized collections that took place in the matters that were not reported to the IOB, similar to our examination of the unauthorized collections that took place in the matters that were reported to the IOB. We found that the field reports of unauthorized collections that were not reported to the IOB did not consistently address whether telephone toll billing records were uploaded into FBI databases. Of the 41 field reports of unauthorized collections that were not reported to the IOB, 19 involved receipt of telephone toll billing records. While 12 of these 19 reports indicated that records were not uploaded into FBI databases, 7 of the reports did not address whether information inappropriately obtained was uploaded into FBI databases.[156]

E. Comparison of Possible NSL-Related IOB Violations Reported to the FBI OGC in 2006 and from 2003 through 2005

To determine whether there were noteworthy trends in the reporting of possible NSL-related intelligence violations to the FBI OGC from 2003 through 2006, we compared the 84 possible intelligence violations reported to the FBI OGC in 2006 with the 26 possible violations reported to the FBI OGC from 2003 through 2005, which we described in our first NSL report.[157] Table 7.4 compares the data in both periods.

As noted above, prior to August 1, 2007, the FBI OGC was not required to report to the IOB instances in which the FBI compounded third party errors such as in this matter. In light of the new reporting standard, the FBI OGC is in the process of reviewing previous adjudications of matters involving third party errors to determine if the FBI compounded these errors. In January 2008, the FBI OGC decided to "rewrite" its initial decision in this matter, and the rewrite concluded that the matter was reportable to the IOB under the new reporting standard because the agent had "inadvertently compounded the third party error by issuing NSLs based on information derived from over-produced data."

[156] The FBI OGC November 16, 2006, guidance memorandum required that improperly obtained information be sequestered pending the FBI OGC's determination of whether the material can be used.

[157] See NSL I, 70.

TABLE 7.4
Comparison of Possible NSL-Related IOB Violations Reported to the FBI OGC (2003 through 2005 and 2006)

Category of Possible IOB Violation	2003 through 2005			2006		
	Possible IOB Violations Reported to the FBI OGC		Possible Violations Reported to the IOB	Possible IOB Violations Reported to the FBI OGC		Possible Violations Reported to the IOB
	FBI Error	Initial Third Party Error		FBI Error	Initial Third Party Error	
Improper authorization	3	0	3	3	0	3
Improper request	4	0	3	3	0	1
Unauthorized investigative activity during lapse in investigation	0	0	0	8	0	1
Unauthorized dissemination	0	0	0	1	0	0
Unauthorized collection	15	4	13	18	52	29
Total FBI or third party errors	**22**	**4**	**19**	**33**	**52**	**34**
Total Possible IOB Violations	**26**		**19**	**85**[158]		**34**

As shown in Table 7.4, the number of possible intelligence violations reported to the FBI OGC rose dramatically in 2006 compared with matters reported in 2003 through 2005, from 26 for the 3 years to 84 in 1 year (2006). The data also shows a marked increase in matters reported involving unauthorized collection.

Overall Number of Violations: The fact that the field reported to the FBI OGC over three times the number of possible intelligence violations in 2006 that it reported for the 3-year period from 2003 through 2005 appears primarily due to a significantly higher incidence of reported third party errors involving unauthorized collection. It also is likely that case agents, supervisors, and CDCs began to more closely scrutinize NSLs and NSL-derived information when the OIG was conducting its first NSL review from December 2005 until March 2007.

Nature of Violations: In 2006, the possible intelligence violations resulting from unauthorized collections were similar to those we reported in our first NSL report, but in 2006, a much higher number of these matters were reported (19 in 2003 through 2005 compared with 70 in 2006). We believe the higher incidence of such reports is attributable to the FBI's closer scrutiny of records obtained in response to NSLs to verify that the

[158] One matter included an initial third party error that resulted in both an unauthorized collection, and an improper request by the FBI. Both possible intelligence violations are reflected in Table 7.4.

responsive data matched the NSL requests. We believe that this heightened scrutiny of adherence to NSL authorities was likely attributable to the FBI's appropriate response to the OIG's first NSL review.

Source of Errors: The increase in the number of reported matters involving third party errors was particularly striking. From 2003 through 2005, FBI errors accounted for 85 percent of the errors, while in 2006 FBI errors accounted for only 39 percent of the errors. With regard to the source of the errors in just the unauthorized collections, from 2003 through 2005, the FBI was responsible for 79 percent of unauthorized collections, while in 2006 the FBI was responsible for only 27 percent of the unauthorized collections. As noted above, this trend suggests that FBI agents, their supervisors, and CDCs were scrutinizing NSLs and NSL-derived information more closely in 2006 than in the past.

Matters Reported to the IOB: While FBI field personnel reported to the FBI OGC in 2006 over three times the number of possible intelligence violations that were reported from 2003 through 2005, the percentage of matters reported to the IOB in 2006 was smaller. From 2003 through 2005, the FBI reported 73 percent of possible intelligence violations to the IOB. In 2006, only 40 percent of the matters reported to the FBI OGC were reported to the IOB. The lower percentage reported to the IOB in 2006 is attributable to the significant number of matters involving unauthorized collections resulting from initial third party errors that the FBI OGC adjudicated after November 13, 2006. After November 13, 2006, under agreement with the IOB, these matters were no longer required to be reported to the IOB.

However, following communications between the FBI OGC and the IOB in August 2007, these matters are now reported to the IOB when the FBI compounds the initial third party error by improperly utilizing the unauthorized information or uploading the unauthorized information into FBI databases. The FBI OGC instructed all CDCs to address whether the initial third party errors were compounded by the FBI when reporting possible intelligence violations to the FBI OGC. The NSLB Deputy General Counsel also advised the IOB's General Counsel that the FBI OGC would review its previous decisions on possible intelligence violations arising from third party errors to determine whether application of the August 2007 directive required further reporting to the IOB. The NSLB's Deputy General Counsel told the OIG that the FBI OGC will adjudicate these matters after the FBI OGC has completed its adjudications of matters arising from the FBI's three 2007 NSL reviews (described in Chapter Three of this report). In light of the increased reporting of initial third party errors, we believe the FBI must take aggressive steps to ensure that when it obtains information not requested in NSLs discrepancies are promptly identified; that records are sequestered, returned, or otherwise handled in conformity with the FBI

OGC's guidance; and that the FBI does not compound the error by using or uploading the improperly provided information.

III. OIG Conclusions and Recommendations

FBI field reports of possible intelligence violations arising from the use of NSLs in 2006 were similar to the reports we examined in our first NSL report covering 2003 through 2005. While there was a notable increase in reports of unauthorized collections in 2006, the percentage of reports of possible intelligence violations attributable to FBI error decreased in 2006. However, in August 2007 the IOB's General Counsel notified the FBI that it would require third party errors to be reported as possible intelligence violations when the FBI compounds such third party errors by utilizing the inappropriately provided information or uploading the information into FBI databases.

We believe the overall increase in the reports of possible intelligence violations may be explained in large part by the attention that our first NSL review focused on the FBI's obligation to examine information obtained in response to NSLs and report possible intelligence violations and to increased scrutiny of NSLs and NSL-derived information by case agents, supervisors, and CDCs.

As discussed in Chapter Two of this report, after the issuance of our first NSL report in March 2007, the FBI and other Department components took a variety of steps to promote compliance with NSL authorities. These include mandatory training of FBI personnel on statutes and rules governing the use of NSLs, as well as several reviews conducted by the FBI's Inspection Division and the National Security Division in conjunction with NSLB attorneys. The FBI also is incorporating technological improvements designed to simplify the preparation of NSL documents and minimize errors in generating these documents. While these efforts are ongoing, we recommend that the FBI:

1. Periodically reinforce in training and guidance provided to case agents and supervisors assigned to national security investigations the FBI OGC directive to report on a timely basis to the FBI OGC possible intelligence violations arising from the use of NSL authorities.

2. 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 they obtain in response to NSLs and to address whether the inappropriately provided information was used or uploaded into FBI databases.

3. 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 the November 30, 2006, FBI OGC guidance memorandum regarding possible NSL-related intelligence violations.

CHAPTER EIGHT:
CONCLUSIONS AND RECOMMENDATIONS

We believe the FBI and the Department have made significant progress in implementing the recommendations from our first NSL report and in adopting other corrective actions to address problems we identified in the use of national security letters. We found that the FBI has devoted significant time, energy, and 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.

For example, the FBI Director and Deputy Director have underscored the significance of the OIG's findings with senior Headquarters officials, Special Agents in Charge (SAC), and other personnel throughout the ranks of the FBI; stressed that compliance with NSL authorities is a major priority; and emphasized that personnel involved in drafting, reviewing, and approving NSLs will be held accountable for infractions. The Deputy Director and the General Counsel have reinforced these messages with SACs and Chief Division Counsels (CDC). The FBI also has generated comprehensive legal guidance on use of NSLs; provided mandatory NSL training to SACs, Assistant Special Agents in Charge, Supervisory Special Agents, Special Agents, Intelligence Analysts, and Headquarters personnel; underscored the responsibility of CDCs in reviewing and approving NSLs and of case agents in ensuring that NSLs do not generate unauthorized records; and developed enhanced information technology tools that should facilitate the preparation of NSLs, reduce or eliminate errors, and improve the accuracy of congressional and public reporting on NSL usage. We believe that these and other steps taken in the last year indicate that the FBI is committed to addressing the problems we identified in our first NSL report.

The FBI's efforts to promote better compliance with NSL authorities also have been enhanced by other FBI initiatives and by the national security reviews conducted by the National Security Division (NSD) and the FBI. The FBI has also created a new Office of Integrity and Compliance (OIC), modeled after private sector compliance programs, to ensure that national security investigations and other FBI activities are conducted in a manner consistent with appropriate laws, regulations, and policies. We believe this office can perform a valuable function by providing a process for identifying compliance requirements and risks, assessing existing control mechanisms, and developing and implementing better controls to ensure proper use of NSLs. However, we recommend that the FBI consider providing the OIC with a larger permanent staffing level so that it can

develop the skills, knowledge, and independence to lead or directly carry out the critical elements of this new compliance program.

In addition to the FBI's efforts to address the OIG's recommendations, the Department's NSD has implemented additional measures to promote better compliance with NSL authorities and to address other issues raised by our first report. For example, in 2007 the NSD began reviews to examine whether the FBI is using various intelligence techniques, including NSLs, in accordance with applicable laws, guidelines, and policies.

In this report, we also examined the FBI's 2007 field and Headquarters NSL reviews, which confirmed that the types of deficiencies identified in our first NSL report had occurred throughout the FBI from 2003 through 2006. The FBI's field review was important because it covered a larger, statistically valid sample of NSLs and case files. The FBI reviews confirmed similar types of possible intelligence violations in the FBI's use of NSLs. However the FBI's field review found a higher overall violation rate (9.43 percent) than the OIG found (7.5 percent) in the sample we examined in our first NSL report.

However, we examined in detail the FBI's reviews and determined that they did not capture all NSL violations in the files they reviewed and therefore did not provide a fully accurate baseline from which to measure future improvement in compliance with NSL authorities. For example, during our re-examination of case files that FBI inspectors determined had no intelligence violations in three field offices, we discovered 15 NSL-related possible intelligence violations. In addition, because FBI inspectors were unable to locate information provided in response to a significant number of NSLs chosen for review in the FBI's random sample, the results of the FBI's field review likely understated the rate of possible intelligence violations.

In its review, the FBI categorized most instances of unauthorized collections as third party errors rather than as FBI errors. Yet, while the initial mistake may have been attributable to NSL recipients who provided more information than was requested in the NSLs, the FBI may have compounded the recipients' error by not taking appropriate steps to identify the overproduction, sequester the information, and report the violation to the FBI Office of the General Counsel (FBI OGC). We also noted that of the 557 identified possible intelligence violations that resulted initially from third party errors, case agents self-reported only 4 (less than 1 percent).

Finally, as required by the Patriot Reauthorization Act, this OIG review examined the FBI's use of national security letters in calendar year 2006.

Our review found that the FBI's use of national security letter requests in 2006 continued the upward trend we identified in our first NSL report, which covered the period 2003 through 2005. In 2006, the FBI issued 49,425 NSL requests, a 4.7 percent increase over NSL requests issued in 2005. For the 4-year period, 2003 through 2006, the FBI issued a total of 192,499 NSL requests.

Most NSL usage (about [redacted] percent of all NSL requests) in 2006 occurred during counterterrorism investigations (compared to [redacted] percent in 2005). About [redacted] percent of all 2006 NSL requests were issued during counterintelligence investigations, and less than [redacted] percent of the requests were generated during foreign computer intrusion cyber investigations. In addition, the use of NSLs in FBI counterterrorism investigations increased from approximately [redacted] percent of investigations opened during 2003 to approximately [redacted] percent of the counterterrorism investigations opened during 2006.

We also found that the percentage of NSL requests related to investigations of "U.S. persons" increased in 2006 compared with the corresponding percentage of such requests in 2005, from 53 percent to 57 percent. We also found that the percentage of NSL requests related to investigations of non-U.S. persons decreased from approximately 47 percent of all NSL requests issued in 2005 to approximately 43 percent of all NSL requests issued in 2006.

With respect to the effectiveness of national security letters, FBI Headquarters and field personnel reported that they continue to believe national security letters are indispensable investigative tools that serve as building blocks in many counterterrorism and counterintelligence investigations. National security letters have various uses, including obtaining evidence to support Foreign Intelligence Surveillance Act applications for electronic surveillance, pen register/trap and trace devices, or physical searches; developing communication or financial links between subjects of FBI investigations and between those subjects and others; providing evidence to initiate new investigations, expand investigations, or enable agents to close investigations; providing investigative leads; and corroborating information obtained by other investigative techniques. FBI officials told us that information derived from NSLs was a significant factor that contributed to the progress of major terrorism and espionage investigations conducted in 2006.

In addition, as required by the Patriot Reauthorization Act, we examined national security letters issued from March 10, 2006, through December 31, 2006, to determine if they were issued without the certification necessary to require the recipients to comply with potentially applicable non-disclosure and confidentiality requirements. The vast

majority of the NSLs and approval ECs we examined substantially complied with the certification requirement and FBI policy. We believe this compliance record was largely due to the prompt guidance the FBI OGC issued on the date the Act was signed, the availability of new NSL forms on its Intranet website, and periodic guidance FBI OGC attorneys provided to the field as questions arose.

Our analysis showed that at least 97 percent of the NSLs we examined in a random sample imposed the non-disclosure and confidentiality obligations on recipients. The majority of the approval memoranda supporting these NSLs asserted that disclosure of the NSLs could prematurely reveal a national security investigation to the targets, persons affiliated with the targets, or the investigative subjects. We found that only 17 of 364 (5 percent) NSL approval memoranda in the random sample contained perfunctory or conclusory justifications for invoking the non-disclosure and confidentiality requirements. While the number of non-compliant NSLs in our random sample was small, we are concerned that some case agents and their supervisors did not follow FBI policy that requires sufficient justification for imposing non-disclosure and confidentiality requirements on NSL recipients.

A small number of NSLs and approval memoranda in our random sample (8 of 375) also contained inconsistent recitals with respect to the need for invoking the non-disclosure and confidentiality obligations, and case agents and their supervisors, as well as CDCs, failed to identify and correct these errors. FBI officials believe that a new NSL data system implemented in 2007 will eliminate this and other data entry discrepancies. However, apart from the random sample, we identified 8 (of the 11) blanket NSLs issued by Counterterrorism Division officials in 2006 that did not comply with the Patriot Reauthorization Act requirements respecting these provisions. These eight NSLs included the pre-Patriot Reauthorization Act language to the effect that the recipient was prohibited from disclosing that the FBI had sought or obtained access to information or records under the *Electronic Communications Privacy Act*. The senior Counterterrorism Division officials who signed these NSLs failed to ensure that the NSLs complied with statutory requirements and that the NSLs and related documents were reviewed by FBI attorneys prior to signing.

As required by the Patriot Reauthorization Act, our review also examined instances of improper or illegal use of national security letters in 2006. First, our review analyzed possible NSL-related intelligence violations that the FBI was required to report to the President's Intelligence Oversight Board (IOB). We identified 84 possible intelligence violations involving the use of national security letter authorities that were reported to the FBI OGC from January 1, 2006, through December 31, 2006, of which 34 were reported to the IOB. These 34 matters included the same types of

intelligence violations reported to the IOB in 2003 through 2005, including NSLs without proper authorization, improper requests, and unauthorized collection of telephone or Internet e-mail records. Of these 34 intelligence violations, 20 were the result of FBI errors, while 14 resulted initially from mistakes by recipients of the national security letters. Of the 84 possible intelligence violations involving the use of NSL authorities identified and reported to the FBI OGC in 2006, the FBI received information it was not entitled to receive in 14 matters. In one of the matters the FBI requested information it was not entitled to under the applicable NSL statute. In the other 13 matters, the FBI made proper requests but, due to third party errors, obtained information it was not entitled to receive under the pertinent NSL statutes.

In sum, despite the significant challenges facing the FBI to eliminate fully shortcomings in its use of NSLs, we believe the FBI and the Department have evidenced a commitment to correcting the problems we found in our first NSL report and have made significant progress in addressing the need to improve compliance in the FBI's use of NSLs. The FBI's executive leadership, including the Director, Deputy Director, and General Counsel, expressed their commitment to ensure that Headquarters and field personnel understand the seriousness of the FBI's shortcomings in its use of NSLs, the proper use of NSLs, and their individual responsibilities for correcting the deficiencies.

However, because only 1 year has passed since the OIG's first NSL report was released and some measures are not fully implemented, we believe it is too early to definitively state whether the new systems and controls developed by the FBI and the Department will eliminate fully the problems with NSLs that we identified. We believe the FBI must implement all of our recommendations in the first NSL report, demonstrate sustained commitment to the steps it has taken and committed to take to improve compliance, implement additional recommendations described in this second report, consider additional measures to enhance privacy protections for NSL-derived information, and remain vigilant in holding FBI personnel accountable for properly preparing and approving NSLs and for handling responsive records appropriately.

As a result, in this report, we make 17 additional recommendations to the FBI to further improve its oversight and use of national security letters. We recommend that the FBI:

1. Create blank mandatory fields in the database supporting the NSL data system 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 result from the current default settings.

2. Implement measures to verify the accuracy of data entry into the new NSL data system by including periodic reviews of a sample of NSLs in the database to ensure that the training provided on data entry to the support staff of the FBI OGC National Security Law Branch (NSLB), other Headquarters divisions, and field personnel is successfully applied in practice and has reduced or eliminated data entry errors. These periodic reviews should also draw upon resources available from the FBI Inspection Division and the FBI's new Office of Integrity and Compliance (OIC).

3. Implement measures to verify that data requested in NSLs is checked against serialized source documents to verify that the data extracted from the source document and used in the NSL (such as the telephone number or e-mail address) is accurately recorded on the NSL and the approval EC.

4. Regularly monitor the preparation of NSL-related documents and the handling of NSL-derived information with periodic reviews and inspections. This includes 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.

5. Assign NSLB attorneys to participate in pertinent meetings of operational and operational support units in the Counterterrorism and Counterintelligence Divisions.

6. Consider increasing the staffing level of the OIC so that it can develop the sufficient skills, knowledge, and independence to lead or directly carry out critical elements of the OIC's work.

7. Reinforce the distinction between the FBI's two NSL authorities pursuant to the *Fair Credit Reporting Act* throughout all levels of 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 Assistant Special Agents in Charge and Special Agents in Charge.

8. Add procedures to include reviews of FCRA NSLs in counterintelligence investigations in the FBI Inspection Division's periodic reviews and in the NSD's national security reviews.

9. Reiterate in its 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.

10. 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.

11. Issue additional guidance addressing the filing and retention of NSL-derived information that will improve the ability to locate NSL-derived information. The guidance should require that all NSL-derived information be appropriately documented, stored, easily identified, and readily available for internal and external review.

12. Include in its routine case file reviews and the NSD's national security reviews an analysis of the FBI's compliance with requirements governing the filing and retention of NSL-derived information.

13. 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 and confidentiality requirements on the NSL recipient.

14. Periodically reinforce in training and guidance provided to case agents and supervisors assigned to national security investigations the FBI OGC directive to timely report to the FBI OGC possible intelligence violations arising from the use of NSL authorities.

15. 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 they obtain in response to NSLs and to address whether the inappropriately provided information was used or uploaded into FBI databases.

16. 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 the November 30, 2006, FBI OGC guidance memorandum regarding possible NSL-related intelligence violations.

We also recommend that the Department:

17. Direct that the NSL Working Group, with the FBI's and the NSD's participation, re-examine measures for (a) addressing the privacy interests associated with NSL-derived information, including the benefits and feasibility of labeling or tagging NSL-derived information, and (b) minimizing the retention and dissemination of such information.

Finally, our forthcoming report will describe in detail the FBI's use of exigent letters, the issuance of 11 improper "blanket" NSLs and other improper NSLs, and other improper requests for telephone records, and will include additional recommendations. Therefore, the FBI should consider the findings and recommendations in our forthcoming NSL report together with the recommendations in this report in addressing measures to continue to improve the FBI's compliance with NSL authorities.

UNCLASSIFIED APPENDIX

The Attorney General
Washington, D.C.

February 29, 2008

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

Dear Mr. Fine:

Thank you for your report entitled "A Review of the FBI's Use of National Security Letters: Corrective Actions and Use in 2006."

When you issued your report last year identifying concerns about the Federal Bureau of Investigation's use of national security letters during the years 2003-2005, Attorney General Gonzales and Director Mueller directed that significant resources be dedicated to improving oversight of this important national security tool. I appreciate your positive assessment of the Department's and the Bureau's efforts in this area, including your conclusion that the Department has made "significant progress" in implementing the recommendations outlined in your report. In particular, I am pleased that your report highlights the Bureau's important work in establishing an Office of Integrity and Compliance and the significant efforts of the National Security Division to create an Oversight Section within the Office of Intelligence, as well as their work to jointly complete 15 national security reviews in FBI field offices and headquarters components in 2007. Your report also correctly emphasizes the need for sustained focus on the Bureau's use of national security letters, and the institutional changes the Department has put in place will help ensure that we continue to devote sufficient resources to the oversight of our national security investigations.

I appreciate your continued recognition that national security letters are an important investigative tool, and that they have contributed to many counterterrorism and counterintelligence investigations. As the substantial efforts of the past year should make clear, the Department is committed to using this critical tool responsibly and in a manner consistent with the law.

Again, my thanks to you and to your staff for your efforts in preparing this report.

Sincerely,

Michael B. Mukasey

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

MAR 07 2008

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

Dear Mr. Fine:

(U) Thank you for providing us a copy of your draft report dated February 14, 2008 titled, "A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006." We have reviewed your report and appreciate the opportunity to provide comment.

(U) As your report makes clear, National Security Letters are an invaluable tool the Federal Bureau of Investigation (FBI) uses to obtain information in national security investigations. We thank you for the extensive review your office has conducted, and look forward to receiving the forthcoming additional recommendations. We believe your report demonstrates the many improvements the FBI and Department of Justice have made to ensure compliance with National Security Letter laws, and applicable guidelines and procedures. While it is critical that our intelligence professionals have the authorities they need to detect and prevent threats to the national security, it is equally imperative that these authorities be executed with due care to the protection of civil liberties and with effective compliance and oversight mechanisms in place.

Sincerely,

J.M. McConnell

U.S. Department of Justice

National Security Division

Washington, D.C. 20530

February 29, 2008

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

Dear Mr. Fine:

Thank you for the opportunity to provide the views of the National Security Division on your report entitled "A Review of the FBI's Use of National Security Letters: Corrective Actions and Use in 2006."

As you know, following the issuance of your initial report identifying concerns about the Federal Bureau of Investigation's (FBI) use of national security letters (NSLs) in 2003–2005, Attorney General Gonzales and Director Mueller directed the implementation of a series of corrective actions, including implementation of all of the recommendations in your initial report. In addition, the Attorney General directed the National Security Division (NSD) and the Department's Privacy and Civil Liberties Office to work with the FBI to implement these corrective actions. These efforts were aimed at ensuring that the FBI uses NSLs in an appropriate manner in compliance with all applicable laws and policy requirements.

This direction and the actions taken pursuant to it, as well as the continuing efforts of the Department, demonstrate the commitment of senior Department leadership to addressing the serious issues identified in your earlier report. As your report notes, the Department has made significant progress and continues to devote significant energy, time, and resources to this effort.

For example, as your report states, the FBI has issued comprehensive guidance concerning the proper use of NSLs and has conducted training in field offices across the country. The FBI has also taken steps to improve the accuracy of its reporting of NSL statistics to Congress by developing a new NSL tracking database that is now available across the FBI. Further, with respect to the use of so-called "exigent letters," the FBI issued a Bureau-wide directive prohibiting the use of the type of letters described in your reports. In addition, in March 2007, the FBI Director ordered a one-time review of ten percent of all national security cases in the 56 FBI field offices and headquarters. This review was a substantial undertaking, requiring the deployment of over 100 inspectors and the review of thousands of investigative files. Finally, as you discuss in your report, the Attorney General requested the Department of Justice's Chief Privacy and Civil Liberties Officer and the Office of the DNI to convene a working group to

examine how NSL-derived information is used and retained by the FBI. The working group has made important progress in this area aimed at the protection of privacy and civil liberties, and the Attorney General has directed the group to continue its efforts. As part of this process, the working group will take into account the recommendations made in your new report.

I also want to highlight the progress of the Department's significant new national security oversight and compliance effort that was publicly announced in July 2007. This effort encompasses substantial changes within the Department of Justice to improve the Department's controls over its national security activities. The effort includes the implementation of a dedicated Oversight Section within NSD and the establishment of an Office of Integrity and Compliance within the FBI. The oversight and compliance programs run by these offices are at the forefront of the Department's ongoing effort to ensure that national security investigations are conducted in a manner consistent with our laws, regulations, and policies, including those designed to protect the privacy and civil liberties of our citizens.

For the first time, DOJ attorneys have been given the clear mandate to examine all aspects of the FBI's national security program for compliance with law, regulations, and policies. As part of this effort, the NSD is conducting regular National Security Investigation reviews at FBI field offices and headquarters units, working with the helpful input of the FBI. These reviews, which were developed in consultation with representatives of the Office of the Inspector General, represent a substantial new level and type of oversight of national security investigations by career Justice Department lawyers with years of intelligence experience. The reviews are not limited to areas where shortcomings have already been identified; instead, they are intended to enhance compliance across the national security investigative spectrum. NSD completed 15 such reviews in 2007 and plans to conduct a similar number on an annual basis. In addition, the Attorney General directed NSD to review all violations that the FBI refers to the Intelligence Oversight Board (IOB) in order to identify recurring problems and to assess the FBI's response to such violations. NSD is reporting regularly to the Attorney General on its review in this area.

The innovations and corrective actions described above reflect a new level of oversight and an appreciation of the need for strong measures to improve compliance in our national security investigations. We appreciate the very fine work that went into this NSL review, and we look forward to working with you as we implement all of the recommendations in your report. As your reports have noted, NSLs are an indispensible investigative tool and have contributed significantly to many counterterrorism and counterintelligence investigations. We are committed to using this critical tool in an appropriate manner that protects the privacy and civil liberties of all Americans.

Sincerely,

Kenneth L. Wainstein
Assistant Attorney General

U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535

February 28, 2008

Honorable Glenn A. Fine
Inspector General
United States Department of Justice
Suite 4706
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Re: U.S. Department of Justice, Office of Inspector General
"A Review of the Federal Bureau of Investigation's Use of National Security Letters: Corrective Actions and Use in 2006"

Dear Mr. Fine:

The FBI appreciates this opportunity to respond to the findings and recommendations made in the Office of the Inspector General's ("OIG's") review of corrective actions taken by the FBI in response to an OIG report published last year regarding the FBI's usage of National Security Letters ("NSLs")("NSL 1") and your review of the FBI's usage of NSLs in 2006 ("NSL 2" or "Report") as required by the USA PATRIOT Improvement and Reauthorization Act of 2005 ("Patriot Reauthorization Act"). This letter conveys our response, and I request that it be appended to the Report.

The Report begins with the first external review that has been conducted of the extensive actions taken by the FBI following the publication of NSL 1 in March 2007 and notes that FBI executive leadership has made correcting the problems identified in NSL 1 a "top priority" (Report at 15). We appreciate the Report's finding that by devoting "significant time, energy and resources," we have made "significant progress" in correcting the deficiencies discussed in NSL 1 (*Id.* at 6). As detailed in the Report, these actions include policy changes, increased mandatory training and the creation of a new NSL automated workflow system that will help ensure compliance with laws, guidelines and policies and will improve the accuracy of our Congressional reporting regarding NSL usage. In addition to the actions recommended in NSL 1, we have conducted extensive internal reviews to ascertain fully the scope and nature of our compliance problems and to guide corrective action. Moreover, we have – in what may be unique within a federal government agency -- created a new Office of Integrity and Compliance ("OIC"), which is modeled after private sector compliance programs. Further, in conjunction with the Department of Justice ("DOJ")'s National Security Division ("NSD"), we have instituted a program of systematic reviews of FBI national security investigations as a way both to ensure compliance with statutory schemes like those that govern NSLs and to serve as a warning system if there are other areas in which our compliance efforts can be strengthened.

Although we have made substantial progress, we concur that we must -- and will -- sustain our commitment to ensuring compliance with the laws and policies governing usage of NSLs.

In addition to providing a review of corrective actions taken in response to NSL 1, the Report also responds to the Congressional mandate that the OIG examine the use of NSLs in 2006. We appreciate the Report recognizing "that the FBI's use of NSLs in 2006 [discussed in the Report] occurred before" NSL 1 and before extensive FBI corrective actions were implemented (Report at 8). Therefore, it is "not surprising[]" that NSL 2 contains findings similar to NSL 1 (*Id.*). NSLs remain an indispensable investigative tool that significantly advance the progress of national security investigations, as the Report details in Chapter 5, and, in almost all cases, potential errors or policy violations involving NSLs relate to information that the FBI was lawfully entitled to obtain (Report at 137).

The Report also reviewed compliance with the non-disclosure and confidentiality provisions of the Patriot Reauthorization Act and found that, thanks to prompt and recurring guidance, the "vast majority" of sampled NSLs (97 percent) complied with the Act in imposing non-disclosure and confidentiality obligations on NSL recipients (Report at 10).

As noted above, the FBI took very substantial corrective actions in the wake of NSL 1, including policy changes, increased mandatory training and the deployment of an automated workflow system for NSLs that is designed to facilitate compliance with statutes, guidelines and policies and to improve the accuracy of the FBI's Congressional reporting. Our most significant actions are discussed below:

- Mandated that all information received in response to an NSL be reviewed prior to uploading the information into FBI databases. Because all reviews of the FBI's NSL usage (*i.e.*, those conducted by FBI and OIG) have found frequent examples of overproduction of materials by NSL recipients, this policy change alone should result in substantially fewer potential intelligence oversight board violations connected to the use of NSLs.
- Prohibited the issuance of exigent letters, and issued clear policy, with audit trails, for acquiring communications records in truly exigent circumstances.
- Prohibited the issuance of NSLs solely from control files.
- Mandated legal review of all NSLs either by attorneys in the Office of General Counsel (OGC) or by Chief Division Counsel and clearly delineated the scope of that review to include the predication for the NSL and the predication for the underlying investigation.
- Established an Office of Integrity and Compliance to facilitate the efforts of executive management to identify and mitigate significant areas of risk. The OIC has been functioning for approximately one year and has demonstrated its value in focusing the attention of executive management on aspects of the FBI's operations and business processes that pose compliance risks.
- In conjunction with DOJ, implemented a program for regular reviews of national security investigations in FBI field offices and headquarters units, including but not limited to compliance with NSL statutes, policies and procedures. Those reviews, like the activities of the OIC, have proved valuable in uncovering policies and procedures that pose compliance challenges.

Following NSL 1, all NSL policies and required procedures were combined into a single document that provides clear and comprehensive guidance to FBI employees who issue and approve NSLs during national security investigations. Prior to its issuance, a draft of the new "one-stop" policy document was briefed to Congressional staff and privacy groups and many of their comments were incorporated into the final version of the policy. We also instituted mandatory in-person NSL training and have developed further training that is available on the FBI's Virtual Academy.

We also developed and fully deployed enhanced information technology tools to automate the NSL workflow, including accumulating the data necessary for Congressional reporting. The system (called the NSL Subsystem) is programmed with drop down menus and other user-friendly features to make the NSL process less time intensive for agents and analysts while simultaneously increasing the accuracy of the process and decreasing the sort of human errors noted by the OIG (*e.g.*, failing to cite the appropriate statute in the Electronic Communication ("EC") requesting an NSL; inconsistency between the data requested in the EC and that requested in the NSL). No NSL can now issue unless vital information is included such as: the subject of the NSL, the predication for the NSL, the type of NSL, the recipient, and the specific targets of the NSL. In other words, the automated system captures all the information required for Congressional reporting before generating the NSL. In addition to improving the accuracy of Congressional reporting, the system ensures that each NSL receives the required legal review and each level of required supervisory review. Providing one database for automated generation of NSLs also reduces the time consuming manual process for generating the required documentation and ensures consistency between the documents reviewed and the NSL actually issued. After a pilot project, the NSL Subsystem became operational in all FBI field offices and Headquarters on January 1, 2008.

Finally, as suggested by the OIG in NSL 1, we issued comprehensive guidance to assist our employees in effectuating the requirement that the FBI use, if possible, the "least intrusive alternative" when conducting investigations. We believe this guidance will be valuable in pointing employees to the sorts of considerations they should balance when deciding between investigative alternatives that have differing levels of intrusiveness.

FBI's Response to Specific Recommendations

Overview: the FBI agrees with all of the OIG's recommendations in the Report and will implement each recommendation as discussed below.

Recommendation #1: Create blank mandatory fields in the software supporting the NSL data system 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 result from the current default settings.

The FBI agrees with this recommendation: To improve the accuracy of NSL Congressional reporting, the FBI will modify the NSL Subsystem to require the user to select one of the U.S. person status options before an NSL may be approved.

Recommendation #2: Implement measures to verify the accuracy of data entry into the new NSL data system by including periodic reviews of a sample of NSLs in the database to ensure that the training provided on data entry to the support staff of the FBI OGC National Security Law Branch, other Headquarters divisions, and field personnel is successfully applied in practice and has reduced or eliminated data entry errors. These periodic reviews should also draw upon resources available from the FBI Inspection Division and the FBI's new Office of Integrity and Compliance (OIC).

The FBI agrees with this recommendation: The FBI agrees that there should be periodic spot checks to ensure that information is being properly reported and to make system improvements where issues are identified. The FBI will utilize the resources of the Inspection Division to conduct such periodic reviews and the resources of OIC to assist in managing the policy and training changes indicated by the results of such reviews. In addition, it is important to note that the data from which Congressional reports will be prepared will come solely from data contained within the NSL Subsystem. Thus, NSL data will no longer be culled from ECs and transferred manually to a standalone database (a process that generated many data entry errors) but instead will be recorded automatically upon the creation of the NSL. As a result, the data entry role of the support staff of the National Security Law Branch is greatly diminished, and the process under the new system is designed to minimize the likelihood of data entry errors.

Recommendation #3: Implement measures to verify that data requested in NSLs is checked against serialized source documents to verify that the data extracted from the source document and used in the NSL (such as the telephone number or e-mail address) is accurately recorded on the NSL and the approval EC.

The FBI agrees with this recommendation: Data such as a telephone numbers or email addresses that are the basis for NSLs should be verified against authoritative documents. Such an authoritative document will frequently, although not always, be a serialized document. The FBI will continue 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.

Recommendation #4: Regularly monitor the preparation of NSL-related documents and the handling of NSL-derived information with periodic reviews and inspections. This includes requiring that during quarterly file reviews, squad supervisors should conduct, at a minimum, spot checks of NSL related documents in investigative files to ensure adherence to NSL authorities, Attorney General Guidelines, and internal policies governing use of NSL authorities.

The FBI agrees with this recommendation: The FBI requires an examination of NSL-related documents and return information during quarterly file reviews. Moreover, the National Security Reviews conducted by DOJ-NSD and FBI-Office of General Counsel ("OGC") will help ensure adherence to laws, policies and procedures with respect to all investigative tools in the national security area.

Recommendation #5: Assign NSLB attorneys to participate in pertinent meetings of operational and operational support units in the Counterterrorism and Counterintelligence Divisions.

The FBI agrees with this recommendation: NSLB will continue the well-established practice of requiring attorneys to attend meetings of operational and operational support units.

Recommendation #6: Consider increasing the staffing level of OIC so that it can develop the sufficient skills, knowledge, and independence to lead or directly carry out critical elements of the OIC's work.

The FBI agrees with this recommendation: The mission of the OIC is to develop, implement, and oversee a program that ensures that there are processes and procedures in place that facilitate FBI compliance with both the letter and the spirit of all applicable laws, regulations, rules and policies. The OIC will cultivate an environment committed to these principles, serve as a focal point for the compliance program, and assist FBI management at all levels in maintaining a culture where ethics and compliance are emphasized as paramount considerations in decisions throughout the FBI.

OIC staff engages the leadership of the FBI in integrating the Integrity and Compliance Program into all FBI operations, programs, and activities and promoting a culture of ethical compliance throughout the FBI. The Office is responsible for establishing policy and methodology for compliance standards, risk assessment, workflow, monitoring and auditing, as well as establishing baseline standards for measuring the effectiveness of risk mitigation measures. OIC's responsibilities also include working with the Inspection Division to develop appropriate inspection protocols and procedures, tasking the Inspection Division with conducting targeted audits as needed, and analyzing the results and recommending such actions as may be necessary or appropriate to mitigate identified risks. OIC is also tasked with developing effective and open channels for receiving reports, including anonymous reports, of potential compliance risks; receiving, reviewing and analyzing data from a variety of sources to identify compliance trends, problems, and best practices; delivering training on the Integrity and Compliance Program; and supporting and facilitating the work of the Integrity and Compliance Council and the Integrity and Compliance Executive Management Committees. OIC also coordinates and manages the FBI Standards of Conduct and Ethics Program to include effecting liaison with the Office of Government Ethics and the DOJ Ethics Office, the review of financial disclosure reports, the initiation and maintenance of ethics education and training programs, and the provision of ethics advice and counsel to individual officers and employees.

The OIC is making steady progress in each of these areas of responsibility, and the office workload is increasing as the program matures. The OIC expects two additional personnel to report in the near future -- one attorney and one Special Agent -- which will bring the office up to its currently-authorized personnel complement. The FBI will continue to evaluate OIC's personnel needs as the program evolves.

Recommendation #7: Reinforce the distinction between the FBI's two NSL authorities pursuant to the Fair Credit Reporting Act (FCRA) throughout all levels of 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 Assistant Special Agents in Charge and Special Agents in Charge.

The FBI agrees with this recommendation: The FBI will continue to train employees involved in the issuance of NSLs on the distinction between FRCAv and FCRAu NSLs. In addition, the new NSL subsystem will not allow a 1681v NSL to be issued from a counterintelligence investigation further ensuring that agents do not use FCRA NSLs contrary to the authorizing statute.

Recommendation #8: Add procedures to include reviews of FCRA NSLs in counterintelligence investigations to the FBI Inspection Division's periodic reviews and the National Security Division's national security reviews.

The FBI agrees with this recommendation: The Inspection Division is currently undergoing a redesign of its inspection process and will incorporate a review of NSLs, to include FCRA NSLs, in the new inspection protocol for NSB programs.

Recommendation #9: Clarify in its continuing discussions with major credit agencies that the credit 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.

The FBI agrees with this recommendation: The FBI continues to have conversations with credit bureaus regarding responses to FCRA NSLs. The credit bureaus have been asked to carefully review NSL requests and to provide only limited credit information in response to a FCRA 1681u NSL request. The appropriate Chief Division Counsels will continue to communicate with the credit bureaus regarding overproduction in response to NSLs. It is important to note that our ability to work collegially with the credit bureaus on an attorney-to-attorney basis has, in recent years, resulted in fewer overproductions by the credit bureaus.

Recommendation #10: 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.

The FBI agrees with this recommendation: Current FBI training and policies identify matters that must be reported to OGC as potential Intelligence Oversight Board (IOB) matters. Following receipt of a report identifying a potential IOB matter, OGC reviews the conduct described in the report to determine whether the IOB must be notified of the reported error. The FBI will continue to provide such training and will update guidance relating to IOB matters as appropriate.

Recommendation #11: Issue additional guidance addressing the filing and retention of NSL-derived information that will improve the ability to locate NSL-derived information. The guidance should require all NSL-derived information be appropriately documented, stored, easily identified, and readily available for internal and external audit.

The FBI agrees with this recommendation: FBI will coordinate any guidance on filing and retention of NSL information with the NSL working group as it continues to consider whether NSL-derived data should be tagged or labeled or otherwise subject to new rules to limit retention or dissemination of NSL-derived data. In addition, the FBI now requires all NSLs, NSL approving ECs, and records produced in response to an NSL to be maintained in a "National Security Letter" subfile of the investigative file.

Recommendation #12: Include in its 90-day case file reviews and the National Security Division's national security reviews an analysis of the FBI's compliance with requirements governing the filing and retention of NSL-derived information.

The FBI agrees with this recommendation: The FBI now requires supervisors to, *inter alia*, examine compliance with requirements governing filing and retention of NSL-derived information during regular quarterly file reviews. In addition, an analysis of compliance with FBI requirements governing the filing and retention of NSL-derived information will occur in connection with the National Security Reviews.

Recommendation #13: 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 and confidentiality requirements on the NSL recipient.

The FBI agrees with this recommendation: The FBI will continue to issue guidance and training materials as appropriate in order to remind employees involved in the issuance of NSLs that the non-disclosure provision of an NSL is not automatic and that a non-disclosure determination must be made for *each* NSL. In addition, the NSL Subsystem has a banner reminding the user that the determination to impose a non-disclosure obligation must be made on a case-by-case basis for each NSL.

Recommendation #14: Periodically reinforce training and guidance provided to case agents and supervisors assigned to national security investigations the FBI OGC directive to timely report to the FBI OGC possible intelligence violations arising from the use of NSL authorities.

The FBI agrees with this recommendation: Current FBI training and policies identify matters that must be reported to OGC as potential IOB matters. Following receipt of a report identifying a potential IOB matter, OGC reviews the conduct described in the report to determine whether the reported error requires notification to the IOB. The FBI will continue to provide training and update guidance relating to IOB matters as appropriate.

Recommendation #15: Require case agents and supervisors assigned to national security investigations to specify in any reports to FBI OGC the precise remedial measures employed to handle any unauthorized information they obtain in response to NSLs and to address whether the inappropriately provided information was used or uploaded into FBI databases.

The FBI agrees with this recommendation: The FBI currently requires remedial measures to be included in the electronic communication that reports to FBI OGC possible intelligence violations. In future training and guidance, the FBI will continue to emphasize the requirement that such remedial measures be included with the reporting EC.

Recommendation #16: 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 the November 30, 2006, FBI OGC guidance memorandum regarding possible NSL-related intelligence violations.

The FBI agrees with this recommendation: The FBI will continue the practice of incorporating anecdotal information regarding common errors in the use of NSLs in its NSL and intelligence oversight board training. The FBI will update examples of common errors in training as new issues arise. In addition, the FBI is hopeful that the NSL Subsystem will greatly diminish the number of errors in the use and issuance of NSLs, many of which came from inadvertent errors, routing mistakes and typographical errors.

Recommendation #17: Direct the NSL Working Group, with the FBI's and the NSD's participation, to re-examine measures for (a) addressing the privacy interests associated with NSL-derived information, including the benefits and feasibility of labeling or tagging NSL-derived information, and (b) minimizing the retention and dissemination of such information.

The Department of Justice and FBI agree with this recommendation: The Attorney General has directed the working group to continue its work.

Sincerely yours,

Robert S. Mueller, III
Director

U.S. Department of Justice

Office of the Deputy Attorney General

Chief Privacy and Civil Liberties Officer

Washington, D.C. 20530

March 7, 2008

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

Dear Mr. Fine:

Thank you for the opportunity to comment on behalf of the National Security Letter (NSL) Working Group, on your report entitled "A Review of the FBI's Use of National Security Letters: Corrective Actions and Use in 2006." We welcome the recommendation in your report and are pleased that you consider the NSL Working Group an appropriate vehicle to continue to examine and develop further safeguards for privacy and civil liberties.

The NSL Working Group worked with dedication and commitment over the past year to strengthen safeguards for individuals' privacy and civil liberties in connection with the FBI's use of NSLs. We believe that your recommendation, combined with the work that the group has already done and will do going forward, will help achieve the goal we all share – to make certain that the FBI is carrying out its vital national security mission under the rule of law and in a manner that protects the privacy and civil liberties of Americans.

As you note in your report, the NSL Working Group analyzed additional protective measures including new minimization procedures for the FBI. To do this, the group examined an array of issues concerning the use, storage, and dissemination of NSL-derived information to include consideration of tagging and labeling, potential retention periods for each category of NSL-derived data, and the privacy concerns associated with the type of information collected. Additionally, the group met with FBI operational, policy, and technology personnel to better understand the operational and technical feasibility of different options. The group has also received feedback from outside privacy advocates. As we move ahead and take on your recommendation, we look forward to sharing with your office greater detail about the NSL Working Group's activities and progress.

Again, we appreciate your recommendation and commit that the NSL Working Group will continue to address these important issues and keep your office informed. We look forward to continuing this important effort to ensure that the FBI's policies and procedures regarding the use of NSLs safeguard privacy and civil liberties in a manner that is consistent with the FBI's critical mission to protect the Nation from threats to our national security.

Sincerely,

Kenneth P. Mortensen
Acting Chief Privacy and Civil Liberties Officer